英汉密码学与网络安全词典

An English-Chinese Dictionary of Cryptography and Cybersecurity

主编　郎永清

主审　封化民

编者　解献芬　张武江　巴雪静　王　玮

刘伟伟　刘　妍　张艳硕

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

VISIT…

LANZAROTE Caliente.com

内 容 简 介

本词典收录密码学与网络安全领域研究、开发、应用和管理等方面的词语5000多条，涵盖密码学、网络安全、代数与数论等学科，以及相应的基础理论体系、技术体系和应用体系方面的常用基本英语词汇、最新术语、缩略语及其汉译，力求做到术语或相关词条概念体系完整、定义表述准确。所有词条均按字母顺序排列，并进行规范与审定。

本词典适合高等院校密码学专业与网络安全相关专业的师生，网络安全、计算机、通信、电子工程等领域的从业人员，以及翻译工作者使用。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

英汉密码学与网络安全词典/郎永清主编. —北京：电子工业出版社，2017.8
ISBN 978-7-121-31866-5

Ⅰ. ①英…　Ⅱ. ①郎…　Ⅲ. ①密码学－词典－英、汉　②计算机网络－网络安全－词典－英、汉　Ⅳ. ①TN918.1－61　②TP393.08－61

中国版本图书馆CIP数据核字（2017）第131019号

责任编辑：富　军　　特约编辑：刘汉斌
印　　刷：
装　　订：
出版发行：电子工业出版社
　　　　　北京市海淀区万寿路173信箱　邮编 100036
开　　本：880×1 230　1/32　印张：7.5　字数：295千字
版　　次：2017年8月第1版
印　　次：2017年8月第1次印刷
定　　价：68.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：fujun@phei.com.cn。

前　言

当今世界，随着互联网技术的不断更新，网络信息安全日益成为全球关注的一个重要议题，也是摆在世界各国面前的紧迫任务。信息安全是国家安全的重要组成部分。密码理论和加密技术是网络安全技术的核心。可以说，没有密码技术就没有网络安全。随着密码学与网络安全学科的迅速发展，有关的新技术、新名词和缩略语等层出不穷，给学习者和研究者带来极大的不便。

本词典收录当前密码学与网络安全领域常用词语 5000 多条，涵盖密码学、网络安全、代数与数论等学科，以及相应的基础理论体系、技术体系和应用体系方面的常用基本英语词汇、最新术语、缩略语及其汉译，突出现代性、实用性和简明性，力求选词实用精练，体现时代特征，例证典型地道，释义简明准确，编排科学合理。

我们在编纂过程中尝试使用语料库辅助词典编纂技术，建成一个密码学英汉摘要平行语料库（Cryptography English-Chinese Parallel Abstract Corpus，CECPAC）。该库的建设目的就是构建一座语言桥梁，旨在通过定量和定性相结合的优势探讨英汉密码学专业词汇及相关术语的词频和翻译特征。英汉平行语料库为词条的翻译提供了良好的数据支撑，极大地提高了本词典编纂的效率。

《英汉密码及网络安全词典》是一本“专科”双语词典。英语术语翻译也不是“直译”，而是尽可能地从汉语的相同学科找出等价的术语。在词汇筛选及翻译过程中，我们采取密码学教师与外语教师合作编写的方式，保证词典的编纂质量。

本词典适合高等院校密码学专业与网络安全相关专业的师生，网络安全、计算机、通信、电子工程等领域的从业人员及翻译工作者使用。

本词典在编纂过程中得到北京电子科技学院领导、科研处、信息

安全系、人文社科部、图书馆的大力支持。教育部高等学校信息安全专业教学指导委员会秘书长封化民教授在百忙之中审定了全部书稿并提出了宝贵的修改意见。李晓明、李梦东、韩妍妍等同志参加了本词典的策划、选材、编译、审校及修改工作。在此一并表示衷心的感谢！

由于编者水平和学识有限，书中难免有不当之处，敬请读者批评指正。

编 者

2017 年 4 月

目　　录

A …… 1
B …… 14
C …… 21
D …… 46
E …… 57
F …… 67
G …… 75
H …… 81
I …… 86
J …… 100
K …… 101
L …… 106
M …… 115
N …… 127
O …… 135
P …… 142
Q …… 162
R …… 166
S …… 178
T …… 205
U …… 216
V …… 220
W …… 223
X …… 227
Y …… 228
Z …… 229

A

A5	一种对称密码算法
AAA	Authentication, Authorization, Accounting 验证、授权和记账
AAC	Advanced Audio Coding 高级音频编码
ABA Digital Signature Guidelines	美国律师协会（American Bar Association）1996 年制定的数字签名指南
Abel	阿贝尔（挪威数学家）
Abelian	阿贝尔的，可交换的
Abelian Varieties	阿贝尔簇
Abreast Davies-Meyer	并列 DM 算法
Absence of Communication Attack	不存在通信攻击
Absolute Indicator	绝对指示器
Abundanceof Communication Attack	大量通信攻击
Abundant Number	过剩数
Abuse-Free Protocol	无滥用协议
Abwehr	（德国第二次世界大战期间）反间谍机关
AC0 Leakage	AC0 泄漏
Access	（使用权）访问
Access Authority	访问授权
Access Control	访问控制
Access Control List	访问控制表
Access Control Mechanism	访问控制机制
Access Control Model	访问控制模型

Access Control Policy	访问控制策略
Access Level	访问级别
Access List	访问列表
Access Management	访问管理
Access Matrix Model	访问矩阵模型
Access Point	访问点，接入点
Access Profile	访问配置文件
Access Right	访问权限
Access Structure	访问结构
Access Type	访问类型
Account	账户
Account Management	账户管理
Accountability	可说明性，责任性，问责制
Accounting Legend Code	记账识别码，计算代码，会计图例编码
Accounting Number	账号
Account Owner	账户拥有者
Accreditation	验证，认可
Accreditation Authority	认证机构
Accreditation Boundary	认证边界
Accreditation Package	认证包
Accrediting Authority	认证机构
Accumulator	累加器
ACE-KEM	NESSIE 选择的非对称密码机制
Acquirer	收单方，收购方
Acrostics	藏头诗，离合文，数行文字
ACS	Access Control Services 访问控制服务
Acting on a Set	作用于一个集合
Action of Group on a Set	一个集合上群的作用
Activation Data	激活数据

Active Adversary	活跃敌手
Active Attack	主动攻击
Active Content	动态内容，活动内容
Active Cryptanalysis	主动密码分析
Active Eavesdropper	主动窃听者
Active Penetration Test	主动渗透测试
Active Security	主动安全
Active Security Testing	动态安全测试
ActiveX	ActiveX 控件
Ad Hoc Network	自组网，自适应网络
Adaptive Adversary	适应性攻击
Adaptive Auxiliary Information (AAIMPC)	自适应辅助信息
Adaptive Chosen Ciphertext Attack	自适应选择密文攻击
Adaptive Chosen Plaintext Attack	自适应选择明文攻击
Adaptively Secure	自适应安全
Adaptively Secure Garbling	自适应安全置乱
Addition Rule	加法规则
Addition Chain	加法链
Addition Problem	加法问题
Addition Sequence	加入顺序
Additional Assumption	额外假设
Addition-Subtraction Chain	加减法链
Additive Group	加法群
Additive Inverse	加法逆元
Additive Knapsack	加法背包
Additive Noise	加性噪声

Additional Decryption Key	附加的解密密钥
Add-on Security	(计算机之外的) 附加保护措施
Address Spoofing	地址欺骗
Adequate Security	足够的安全 (保障) 性
A-Distance	A 距离
Adjoint	共轭，伴随矩阵
Adjoint Matrix	伴随矩阵
Adleman-Pomerance-Rumely Primality	Adleman、Pomerance 和 Rumely 的素性测试
Administrator	管理员
Administrative Account	管理 (员) 账户
Administrative Safeguard	管理保障
Admissible Change of Variables	变量的容许变化
Advanced Encryption Standard	高级加密标准
Advanced Key Processor (AKP)	高级密钥处理程序
Advanced Persistent Threats (APT)	高级持续性威胁
Advantage	优势
Adversarial Challenge	敌手的挑战
Adversarially-Chosen Plaintext Distribution	敌手选择明文分布
Adversary	敌手
Adversary Structure	攻击结构
Adversary Simulator	咨询模拟器
AE	Authenticated Encryption 认证加密
AEAD	Authenticated Encryptionwith Associated Data 带关联数据的认证加密

AES	Advanced Encryption Standard 高级加密标准
Affine Equivalent	仿射等价
Affine Function	仿射函数
Affine Invariant	仿射不变量
Affine Scheme	仿射概形
AG-Code	Algebraic Geometry Code 代数几何码
Agency	代理
Agency of Certification Authority	数字证书授权机构
Agent	代理人
Aggressive Mode	积极（进攻）模式
AGM Method	基于代数几何的算法
AH	Authentication Header 身份验证报头
AKP	Advanced Key Processor 高级密钥处理程序
Alberti Encryption	Alberti 加密
Alberti Table	Alberti 表格
Alert	报警，警告
Alert Message	警报信息
Algebraic Attack	代数攻击
Algebraic Degree	代数次数
Algebraic Element	代数元
Algebraic Immunity	代数免疫性
Algebraic Independence	代数独立性
Algebraic Integer	代数整数
Algebraic Normal Form	代数范式，代数标准型
Algebraic Number	代数数
Algebraic Number Field	代数数域

Algebraic Reduction	代数归约
Algebraically Closed	代数封闭的
Algebraically Independent Element	代数无关的元素
Algebraic-Geometry Code	代数几何码
Algebra	代数
Algorithm	算法
Aliquot Cycle	循环圈，真因子圈
All-But-One Decryption	可重复性解密
All-But-One Simulation Technique	可重复性仿真技术
All Hazards Approach	全致灾因子方法
Allocation	配置
All-or-Nothing Encryption	全有全无加密术
Almost Bent Function	几乎 Bent 函数
Almost Perfect Nonlinear Function	几乎完全非线性函数
Almost Perfect Zero-Knowledge	几乎完全零知识
Alternate	交替，轮流
Alternate COMSEC Custodian	替补通信安全管理人员，备用 COMSEC 保管人
Alternate Site	备用站点，备用处理设施
Alternate Work Site	临时工作地点，交替工作站点
Alternating Group	交替群
Alternating Step Generator	一般步进生成器
American Bar Association	美国律师协会
American National Institute of Standards and Technology (NIST)	美国国家标准与技术研究所

Amicable Pair	亲和数对
Amitsur Levitzki Theorem	Amitsur Levitzki 定理
Application Recovery	应用程序恢复
Amortized Communication Complexity	消减通信复杂度
Amortized Cost	摊销成本
Amplified Boomerang Attack	放大 Boomerang 攻击
An Apriori Bounded Polynomial Number	一个先验界多项式数目
An Interval in a Modular Lattice	模格的一个间隔
Analogue	类似物
Analogue for Algebra	模拟代数
Analogue for Ring	模拟环
Analysis	分析
Analytic Number Theory	解析数论
AND Function	AND 函数
Anisotropic	各向异性
Anisotropic Kernel	各向异性核
Annihilator	零化子
Anomalous Binary Curve	异常二进制曲线
Anomaly	异常
Anomaly-Based Detection	异常检测
Anonym	匿名者
Anonymity	匿名
Anonymity Set	匿名集
Anonymous Broadcast	匿名广播
Anonymous Network	匿名网络
Anonymous Remailer	匿名（重游程序）转发器

Anonymous Signature	匿名签名
ANSI	American National Standards Institute 美国国家标准学会，ANSI 编码
Antihomomorphism	反同态，反同构
Anti-Jam	抗干扰
Anti-Linear	抗线性
Anti-Spoof	反欺骗
Antispyware Software	反间谍软件
Antivirus Software	防病毒软件
APN Function	APN 函数
APPEL	P3P 偏好交换语言
Applicant	申请人
Application	应用程序
Application Cryptogram	应用密文
Approval to Operate（ATO）	批准运行
Approved Modeof Operation	认可的操作模式
Approved Security Function	核准的安全功能
Approximate Common Divisor	近似公因子
Approximate Eigenvector	近似特征向量
Approximation	近似（算法）
APT	Advanced Persistent Threats 高级持续性威胁
Arbitrary Auxiliary Information	任意辅助信息
Arbitrary Communication Resource	任意通信资源
Arbitrary Cyclotomic	任意单位根
Arbitrary Key	任意密钥
Arbitrary Partial Information	任意部分信息

Arbitrary Permutation	任意置换
Archimedes	阿基米德
Archive	存档，档案文件
Arithmetic	算术
Arithmetic Fundamental Theorem	算术基本定理
Arity	参数数量
ARQC	Authorization Request Cryptogram 授权请求密文
Artin Chevalley Theorem	阿廷·谢瓦莱定理
Artin's Conjecture	阿廷猜想
ARX	Addition，Rotation and XOR 加、循环移位和异或结构
AS	AS 运算符
Ascending Chain	上升链条，上升链
Assessment	评价，评估
Assessment Finding	评估结果
Assessment Method	评估方法
Assessment Object	评估对象
Assessment Objective	评估目标
Assessment Procedure	评估程序
Assessor	鉴定器，评定器，评审员
Asset	资产
Asset Criticality	资产临界点
Asset Identification	资产鉴定
Asset Reporting Format（ARF）	资产报告格式
Associated Data	关联数据
Associative	联想的，组合的，联合的
Associative Law	结合律

Associativity	关联性
Associator	相伴，伙伴
Assumption	假设，设想
Assurance	确保，确信度，保障
Assurance Case	安全保证案例，保障案例
Assured Information Sharing	确保信息共享
Assured Software	有保证的软件
Asymmetric	非对称
Asymmetric Cryptography	非对称加密学
Asymmetric Cryptosystem	非对称密码系统
Asymmetric Functionality	非对称功能
Asymmetric Key	非对称密钥
Asymmetric Proxy Encryption	非对称代理加密
Asymmetric Proxy Signature Scheme	非对称代理签名方案
Asymmetric Watermarking	非对称水印
Asymptotic Complexity	渐近复杂度
Asymptotic Security	渐近安全性
Asymptotically	渐近性
Asymptotically Optimal	渐近最优
Asymptotically Square Root	渐近平方根
Asymptotically Tight Security Analysis	渐近紧致安全分析
Asynchronous Self-Synchronizing	异步式自同步
ATM	Asynchronous Transfer Mode 异步传输模式
ATO	Approval to Operate 批准运行
Attack	攻击
Attack Sensing and Warning (AS&W)	攻击监测和警告

Attack Signature	攻击签名
Attribute	属性
Attribute Authority	属性授权，属性权威
Attribute Certificate	属性证书
Attribute Management	属性管理
Attribute-Based Access Control	基于属性的访问控制
Attribute-Based Authorization	基于属性的授权
Attribute-Based Encryption	基于属性的加密
Attribute-Based Encryption Scheme	基于属性的加密方案
Auctioneer Role	拍卖者角色
Audit	审计，审核
Audit Data	审计数据
Audit Log	审计日志
Audit Protocol	审计协议
Audit Reduction Tool	审计工具还原，审计精选工具
Audit Review	审计复核
Audit Trail	审计跟踪
Authenticate	认证
Authenticated Data	认证数据
Authenticated Encryption	认证加密
Authenticated Encryption with Associated Data	带相关数据的认证加密
Authenticated Key Exchange	认证密钥交换
Authentication	认证
Authentication Authority	认证授权
Authentication Information	认证信息
Authentication Code	认证码

Authentication Header	认证报头
Authentication Mechanism	认证机制
Authentication Mode	认证模式
Authentication Period	认证周期
Authentication Protocol	认证协议
Authentication Provider	认证提供者
Authentication Scheme	认证方案
Authentication Server	认证服务器
Authentication Tag	认证标签
Authentication Token	认证令牌
Authenticator	认证者，鉴定符
Authenticity	认证性，可靠性
Authenticity Proof	鉴别证明
Authenticode	授权认证码
Authority	权威，权限
Authorization (to operate)	授权运行
Authorization Algebra	授权代数
Authorization Architecture	授权体系结构
Authorization Boundary	授权范围
Authorization Management	授权管理
Authorization Policy	授权策略
Authorize Processing	授权处理
Authorized User	授权用户
Authorized Vendor	授权供应商
Authorized Vendor Program (AVP)	授权供应商程序
Authorizer	授权人
Authorizing Official	官方授权
Authorizing Official Designated Representative	官方指定授权代表

Auto Key	自动密钥
Auto Reducibility	自动归约
Auto-Correlation	自动相关，自相关
Automated Key Transport	自动密钥传输
Automated Password Generator	自动口令生成器，自动密钥生成器
Automated Security Monitoring	自动安全监测
Automated Teller Machine	自动柜员机
Automatic Clearing House	自动（票据交换）清算所
Automatic Remote Rekeying	自动远程密钥更新
Automatic Search Tool	自动搜索工具
Automatic Template Analysis	自动模板分析
Automorphism	自同构
Autonomous System（AS）	自治系统
Autoreducibility	自还原理念
Auxiliary Information	辅助信息
Auxiliary Input	辅助输入
Auxiliary Input Model	辅助输入模型
Auxiliary Security Parameter	辅助安全参数
Availability	可用性
Avalanche	雪崩
AVP	Authorized Vendor Program 授权供应商程序
Awareness（Information Security）	信息安全意识，知晓性

B

Bezout Number	贝祖定理，Bezout 数
Baby-Step Giant-Step Method	小步大步法
Backdoor	后门程序，后门
Backtracking Resistance	回溯阻力
Backup	备份
Backward Security	后向安全
Backwards Mixing	后向混合
Bad Prime	不好的素数
Balance Property	平衡特性
Ball Collision	球碰撞
Bandwidth	带宽
Banner	标志，横幅，旗帜
Banner Grabbing	标志获取
Bare Public-Key Model	单纯公钥模型
Base	基，库，基数
Base Key	基础密钥，基本键
Base of Index	指标的基，指数基
Baseline	基线
Baseline Configuration	基线配置
Baseline Security	安全基线
Baselining	基线监测
Basic Constraints Extension	基本限制扩展
Basic Merkle-Hellman Scheme	Merkle-Hellman 基础方案
Basic Testing	基础测试

Bass-O-Matic	一种新型加密算法
Bastion Host	堡垒主机
Batch Factoring	批量构造，批量分解
Batch Fully Homomorphic Encryption Scheme	分批全同态加密方案
Batch-Wise Multiplication Verification	分批的乘法验证
BCH Code	Bose Chaudhuri Hocquenghem 编码，一种重要的纠错码
BCM	Body Control Module 车身控制模块，Business Continuity Management 业务连续性管理
BDH Assumption	BDH 假设
Beaufort Encryption	博福特加密
Beaufort Table	博福特表格
Behavioral Outcome	行为结果
Bell Measurement	贝尔测量
Bell State	贝尔态
Benign Environment	良性病毒环境，温和环境
Bent Function	Bent 函数
Berlekamp Q Matrix	Berlekamp Q 矩阵
Berlekamp-Massey Algorithm	Berlekamp-Massey 算法
Beyond-Birthday-Bound Security	超越生日界的安全性
BGMW Method	BGMW 方法
BGP	Border Gateway Protocol 安全边界网关协议
BIA	Business Impact Analysis 商业影响分析
Bias	误差，偏差

Biased Coin Flip	偏掷硬币
Biclique	二元组，双团
Bicomposite	双复合
Big-Oh Notation	大 O 表示法
Big-Omega (Ω)	大 Ω
Bigram	二元语法，双字母组
Bigram Substitution	二元语法代换
Big-Theta (θ)	大 θ
Bijective	(函数、关系) 双射的
Bilinear	双线性的
Bilinear Form	双线性形式
Bilinear Diffie-Hellman Problem	双线性 Diffie-Hellman 问题
Bilinear Elliptic Curve	双线性椭圆曲线
Bilinear Group	双线性群
Bilinear Pairing	双线性映射，双线性对
Bilinear Radical	双线性基
Bill of Lading	提货单
Bimodal Gaussian	双模态高斯
Binary Alphabet	二进制字母表
Binary Curve	二进制曲线，二元曲线
Binary Euclidean Algorithm	二进制欧几里德算法
Binary Expansion	二元展开
Binary Exponentiation	二进制求幂运算
Binary Field	二元域
Binary GCD Algorithm	二进制 GCD 算法
Binary Linear Code	二元线性码
Binary Random Code	二进制随机码
Binder	连接器

Binding	绑定，连接
Binet's Formula	比内公式
Binomial Coefficient	二项式系数
Binomial Distribution	二项分布
Binomial Theorem	二项式定理
Biometric	生物计量
Biometric Identification	生物特征认证
Biometric Information	生物特征信息
Biometric System	生物特征系统
Biometrics	生物测量学，生物统计学
Bipartite Substitution	双边替换
Birthday Attack	生日攻击
Birthday Bound	生日界限
Birthday Paradox	生日悖论
Bit	比特
Bit Error Rate	比特误码率
Bit Generator	比特发生器
Bit Tracing	比特追踪
Bit Slice	比特切片
Black Box Testing	黑盒测试
Black Core	黑核
Black-Box	黑盒，黑箱
Black-Box Attack	黑盒攻击
Black-Box Reduction	黑盒归约
Black-Box Simulator	黑盒模拟器
Black-Box Tracing	黑盒追踪
Blacklist	黑名单
Blacklisting	被列入黑名单
Blended Attack	混合攻击

Blind Signature	盲签名
Blind Watermarking	盲水印
Blinding Factor	盲化因子
Blinding Technique	盲化技术
Block Cipher	分组密码
Block Cipher Algorithm	分组加密算法
Block Code	分组码
Block Korkine-Zolotarev Reduction	BKZ 规约
Block Length	分组长度
Blowfish	双鱼算法
BLS Short Digital Signature	BLS 短数字签名
Bluetooth	蓝牙
Bluetooth Encryption	蓝牙加密
Blum Integer	Blum 整数
Blum Prime	Blum 素数
Blum-Blum-Shub Pseudorandom	Blum-Blum-Shub 伪随机
Blum-Goldwasser Public Key Encryption System	Blum 和 Goldwasser 公钥密码体制
Bodyof Evidence (BOE)	证据主体
Boneh-Durfee Attack	Boneh-Durfee 攻击
Boneh-Franklin Identity Based Cryptosystem	Boneh-Franklin 基于身份的加密系统
Boolean	布尔的
Boolean Algebra	布尔代数
Boolean Circuit	布尔电路
Boolean Formula	布尔公式
Boolean Function	布尔函数

Boolean Query	布尔查询
Boolean Ring	布尔环
Boolean Variable	布尔变量
Boomerang Attack	Boomerang 攻击，回旋镖攻击
Bootstrapping Procedure	自展程序，自举程序
Bootstrapping Theorem	自举定理
Bot	机器人程序
Botnet	僵尸网络
Bound	界
Bound for P-Defect	P 亏量的界
Boundary	边界
Boundary Protection	边界防护
Boundary Protection Device	边界防护装置
Bounded Collusion	有界限共谋
Bounded Leakage	有界泄漏
Bounded Player Model	有界选手模型
Bounded Variant	有界变量
Bounded-Concurrent	有界并发
Bounded-Degree Function	有界次数函数
Bounded-Input-Length	有限输入长度
Box Principle	抽屉原理
Braid Group	辫群
Branch Number	分支数
Brickell Low Density Attack	Brickell 低密度攻击
Brickell Merkle-Hellman Attack	Brickell Merkle-Hellman 攻击
Bridge Certification Authority	基于桥方式认证机构
Broadcast Channel	广播信道
Broadcast Encryption	广播加密

Broad Remote Access	宽带远程接入
Brute Force Attack	暴力（穷举）攻击
Brute Force Password Attack	暴力口令破解
Budan's Theorem	布当定理
Buffer Overflow	缓冲器溢出
Buffer Overflow Attack	缓冲器溢出攻击
Bulk Encryption	整批加密，批量加密
Burmester-Desmedt Protocol	Burmester-Desmedt 协议
Business Continuation	业务连续性
Business Continuity Management (BCM)	业务连续性管理
Business Continuity Plan (BCP)	业务连续性计划
Business Impact Analysis (BIA)	业务影响分析
Business Interruption	业务中断
Business Interruption Cost	业务中断代价
Business Recovery Critical Path	业务恢复的关键路径
Business Unit Recovery	业务单元恢复
Butterfly Algorithm	蝶算法
Buyer Role	买方角色
Byte	字节

C

CA	Certificate Agency 认证机构
Caesar Cipher	凯撒密码
Calculus	微积分
Call Back	回调，回叫
Camellia	一种为许多组织所推崇的分组密码（Block Cipher）
Canadian Trusted Computer Product Evaluation Criteria	加拿大可信计算机产品评估标准
Canceling Property	消去特性
Cancellation Law	消去律，相消律
Candidate Multilinear Map	候选多重线性映射
Canister	密钥保护/发送包
Canonical Matrices	正则矩阵
Canonical S-Expression	典型 S 表达式
Capability	权能，能力
Capability List	能力表
Capstone	顶点
Capstone Policies	顶点规则
Capture	（身份）采集
Captured Agent Trust	捕获执行信任
Card Issuer	发卡单位
Card Shuffle	洗牌
Cardano's Formula	卡丹诺公式
Cardholder	持卡人
Cardinal Number	基数，基数词

Cardinality	基数
Carmichael Number	卡迈克尔数
Cartan-Brauer-Hua Theorem	Cartan-Brauer-Hua 定理
Cartan-Dieudonne Theorem	Cartan-Dieudonne 定理
Cartesian	笛卡儿的，笛卡儿数学思想的
Cartesian Product	笛卡儿积
Cascade Cipher	级联密码
Cascade Encryption	级联加密
Cascading	（信息由上层安全系统向下层的）传递，传达，级联
Cascading Revocation	级联撤销
Cascading-Based Construction	基于级联的结构
CAST	CAST（C. Adams 和 S. Tavares）密码
Casus Irreducibility	Casus 不可约
Category	级别分类，范畴
Cattle Problemof Archimedes	阿基米德牛群问题
Cauchy Sequence	柯西序列
Cayley Graves	八元数
Cayley's Theorem	凯莱定理
CBC/MAC	Cipher Block Chaining 密码分组链接/Message Authentication Code 消息认证码
CC	Common Criteria 通用标准
CCA2	Chosen-Ciphertext Attack 2 主动选择密文安全
CCA2 Secure Cryptosystem	CCA2 安全加密系统
CCIT2	CCIT2 密码
CCM	Combined Cipher Machine 联合密码机
CCR	Complementary Circulating Register 补轮换移位寄存器

CDA	Combined Data Authentication 组合数据认证
CDH	Computational Diffie-Hellman 可计算性 Diffie-Hellman 问题
CDMA	Code-Division Multiple-Access 码分多址
Central Authority	中枢机关
Central Log Management System	中央日志管理系统
Central Office of Record (COR)	(通信安全) 记录中央办公室，中央档案处
Central Services Node (CSN)	中央服务节点
Centralized System	集中式系统
Centralizer	中心化子，定中心器
CEPS-Standard	Common Electronic Purse Specifications Standard 公用电子钱包规格标准
Certificate	证书
Certificate Extension	证书延期
Certificate Management	证书管理
Certificate Management Authority (CMA)	证书管理机构
Certificateof Primality	素性证书，素数证书
Certificate Policy (CP)	证书策略
Certificate Policy Statement	证书策略说明
Certificate Practice Statement (CPS)	电子认证业务规则，认证实务准则
Certificate Revocation	证书吊销
Certificate Revocation List (CRL)	证书吊销列表
Certificate Status Authority	证书核实机构

Certificate-Related Information	证书相关信息
Certification	认证
Certification Analyst	认证分析员
Certification Authority（CA）	认证机构
Certification Authority Facility	认证体系
Certification Authority Workstation（CAW）	认证工作站
Certification Package	认证服务套餐，认证包
Certification Practice Statement（CPS）	认证报告
Certification Test and Evaluation（CT&E）	认证检测与评估
Certified Mail	认证邮件，保证邮件
Certified Trapdoor Permutation	认证陷门置换
Certifier	认证人员
CFB	Cipher Feedback 密码反馈
CFRAC	Continued Fraction Method 连分数法
CGI	Common Gate Interface 公共网关接口
Chain of Custody	监管链
Chain of Evidence	证据链
Chaining Attack	链攻击
Chaining Variable	链接变量
Challenge and Reply Authentication	挑战与应答认证
Challenge Ciphertext	挑战密文
Challenge Covertext	挑战掩饰
Challenge-Response Protocol	挑战与应答协议
Channel Capacity	信道容量

Characteristic Function	特征函数
Characteristic Polynomial	特征多项式
Characterization	特征描述
Chaum Blind Signature Scheme	Chaum 盲签名方案
Chaum-Van Antwerpen Undeniable Signature Scheme	Chaum-Van Antwerpen 不可否认签名方案
Check Word	检验字
Check Sum	校验和
Chief Information Officer (CIO)	首席信息官
Chief Information Security Officer (CISO)	首席信息安全官
Chinese Remainder Theorem	中国剩余定理，孙子剩余定理
Chord-and-Tangent Rule	弦切法则
Chor-Rivest Cryptosystem	Chor-Rivest 密码系统
Chosen Ciphertext Attack	选择密文攻击
Chosen Message Attack	选择消息攻击
Chosen One-out-of-Two	二选一
Chosen Plaintext and Ciphertext Attack	选择明文及密文攻击
Chosen Plaintext Attack	选择明文攻击
Chosen Related Key Attack	选择相关密钥攻击
Chosen-Ciphertext Security	选择密文安全性
Chromatic	平均律
CIA	Confidentiality, Integrity and Availability 机密性、完整性和可靠性
Cipher	密码
Cipher Block Chaining-Message Authentication Code (CBC-MAC)	密码分组链接消息认证代码

Cipher Feedback	密码反馈模式
Cipher Suite	密码组合，密码套件
Cipher System	密码系统
Cipher Text Auto-Key (CTAK)	密文自动密钥
Ciphertext	密文，加密文本，密码报文
Ciphertext Attack	密文攻击
Ciphertext Boundary Hiding	密文边界隐匿
Ciphertext Compromise	密文泄露
Ciphertext Delegation	密文授权
Ciphertext Fragmentation	密文碎片
Ciphertext Only Attack	唯密文攻击
Ciphertext Secure	密文安全
Ciphertext Stealing	密文盗用
Ciphertext Expansion	密文扩展
Ciphertext-Policy Attribute-Based Encryption Scheme	基于密文策略属性加密方案
Ciphony	密码电话，密码电话学
Circle	圆，圈
Circuit Complier	电路编译器
Circuit-Description Complexity	电路描述复杂性
Circular Shift	循环移位
Circumvent	规避，欺诈，用计谋战胜
CISO	Chief Information Security Officer 首席信息安全执行官
Claimant	申请人，索赔人，原告
Class Equation	类方程
Class Field Theory	类域论
Class Number	类数

Classical Cryptosystem	传统密码体制
Classical Leftover Hash Lemma	经典剩余散列引理
Classical RSA-Based Cryptographic System	经典 RSA 加密系统
Classified Information	机密信息
Classified Information Spillage	机密信息泄露
Classified National Security Information	机密国家安全信息
Claw-Free	无爪的
Cleartext	明文
Clearance	许可权
Clearance Level	许可证级别
Clearing	清除
Client (Application)	客户（应用程序）
Client Hello	客户问候消息
Client-Server Setting	客户端服务器设置
Clinger-Cohen Act of 1996	克林格和科恩法案（1996）
Clipper	Clipper 加密芯片
Clip Scheme	Clip 方案
Clock-Controlled Generator	钟控序列发生器
Closed Security Environment	封闭安全环境
Closed Storage	封闭存储
Closest Vector Problem	最近向量问题
Close-to-Optimal	接近理想的
Closure	封闭，闭包
Closure Alert	封闭警报
Closure Attack	封闭攻击
Cloud Computing	云计算

Cloud Storage	云存储
Cloud-Assisted Computation	云辅助计算
CMA	Chosen Message Attack 选择消息攻击
CMAC	CMAC 算法（CMAC = Cipher-based Message Authentication Code）
CMP	Core Messaging Platform 核心报文处理平台
CMS	Cryptographic Message Syntax 加密消息语法
Coalition	联盟，共谋
Coarse Grained	粗纹理的，粗颗粒的
Cock's Identity Based Cryptosystem	柯克的基于身份加密体制
Code	码，纠错码，代码
Code-Based Cryptosystem	基于纠错码的密码体制
Code Book	密码本
Code Group	码群，代码组
Code Vocabulary	密码表
Codebook Attack	代码本攻击
Code Division Multiple Access	CDMA 码分多址
Codeword	码字，代码字
Codeword Symbol	码字符号
Coding Theory	编码理论
Codomain	值域
Coefficient	系数
Cofactorization	辅因子分解，余因子分解
Cogredient	同步的
Cohen-Lenstra-Bosma Algorithm	Cohen-Lenstra-Bosma 算法
Coherence	相干性，连贯性
Cohomology	上同调
Cold Boot Attack	冷启动攻击

Cold Site	冷站点，冷备援中心
Cold Start	冷启动
Collective Noise	集体噪声
Collective-Dephasing Channel	集体退相干信道
Collective-Rotation Channel	集体旋转信道
Collision	碰撞
Collision Attack	碰撞攻击
Collision Freeness	无碰撞
CollisionIntractable	碰撞困难的
Collision Resistance	抗碰撞
Collision Resistant	抗碰撞的
Collision Security Proof	碰撞安全性证明
Collision-Resistant Hash Function (CRHF)	抗碰撞哈希函数
Collusion Attack	共谋攻击
Collusion-Free Protocol	无共谋的协议
Collusion-Preserving Computation	保持共谋计算
Collusion-Resistant Broadcast Encryption	抗共谋广播加密
Combination Number	组合数
Combination Generator	组合生成器
Combinatorial Search Problem	组合搜索问题
Combined Data Authentication	组合数据验证
Combined Mode	组合模式
Combiner	合成器，组合生成器
Command Authority	命令授权，命令权限
Commensurable Number	可比数值，比例数
Commercial COMSEC Evaluation Program (CCEP)	商业通信安全评估体系

Commit Phase	提交阶段，承诺阶段
Commitment	提交，承诺，保证
Commitment Scheme	承诺方案
Common Access Card (CAC)	通用访问卡，通用存取卡
Common Carrier	公用载波，共用载子，共通传输网，公共通信企业
Common Configuration Enumeration (CCE)	通用配置枚举
Common Configuration Scoring System (CCSS)	通用配置评分系统
Common Control	公共控件，通用控件
Common Control Provider	公共控件提供方
Common Criteria	通用标准
Common Electronic Purse Specification	公用电子钱包规格
Common Fill Device	通用（读入、转换等）设备
Common Misuse Scoring System (CMSS)	常见误用评分系统
Common Platform Enumeration (CPE)	通用平台列举
Common Reference String (CRS)	公共参考串
Common Vulnerabilities and Exposures (CVE)	通用漏洞列表
Common Vulnerability Scoring System (CVSS)	通用安全漏洞评分系统
Communication Channel Anonymity	通信信道匿名性
Communication Complexity	通信复杂性，通信复杂度

Communications Cover	通信隐藏
Communications Deception	通信欺骗
Communications Profile	通信配置文件
Communications Security (COMSEC)	通信安全
Community of Interest (COI)	利益同盟，利益共同体
Community Risk	公共危险
Commutative	交换的
Commutative Group	交换群
Commutative Matrix	交换矩阵
Commutativity	交换性
Commutator	换向器，整流器
Commutator (Derived)	(衍生) 转接器
Comp128-1	Comp 128-1 算法
Compact Ciphertext	紧致密文
Compact Proof	紧致证明
Compact Share	紧凑份额
Companion Matrix	伴随矩阵，相伴矩阵
Comparison	比照，辨识
Comparison Theorem of Maurer	Maurer 比较定理
Compartmentalization	分隔，划分
Compartmented Mode	分隔模式
Compensating Control	补偿控制
Compensating Security Control	补偿安全控制
Compiler	编译器
Complement	补集，补
Complementary Circulating Register	补轮换移位寄存器

Complete Context Hiding Security	完整语境隐藏安全性
Complete Functionality	完整的功能
Complete Mediation Property	完全调节属性
Completeness	完整性，完备性
Complex Multiplication	复乘法
Complex Number	复数
Complex Plane	复平面
Complexity Class	复杂性类
Complexity Leveraging Argument	复杂性泄露论证技术
Complexity Spectrum	复杂性谱系
Complexity Theory	复杂性理论
Composable Protocol	可复合协议
Composite	复合
Composite Arithmetic	复合运算
Composite Degree	复合次数
Composite Number	合数
Composite Order	合数阶
Composite Residuosity Assumption	复合剩余假设
Composition Series	组成列，合成列
Compound	复合
Comprehensive Testing	综合检测
Compression Function	压缩函数
Compromise	泄露（信息）
Compromising Emanation	泄密发射
Compton Effect	康普顿效应，亦称 Compton-Debye Effect
Computable Function	可计算函数

Computerized Information Resource	计算机信息资源
Computation	计算
Computation Protocol	计算协议
Computational Complexity	计算复杂度
Computational Complexity Theory	计算复杂性理论
Computational Cost	计算消耗
Computational Diffie-Hellman	计算 Diffie-Hellman 问题
Computational Entropy	计算熵
Computational Hardness	计算困难性
Computational Intractability Assumption	计算困难性假设
Computational Security	计算安全性
Computational Soundness	计算正确性
Computational Zero-Knowledge	计算零知识
Computationally Bounded	计算有界的
Computationally Invertible Information	计算可逆信息
Computationally Secure Steganography	计算安全隐写术
Computationally Sound Proof System	计算的正确证明系统
Computationally-Sound	计算正确的
Computationally-Unbounded	计算能力不受限制的
Computer Abuse	计算机滥用
Computer Cryptography	计算机密码学
Computer Forensics	计算机取证
Computer Incident Response Team（CIRT）	计算机事件反应组

Computer Network Attack (CNA)	计算机网络攻击
Computer Network Defense (CND)	计算机网络防御
Computer Network Exploitation (CNE)	计算机网络开发，计算机网络利用
Computer Network Operations (CNO)	计算机网络对抗
Computer Security (CompuSec)	计算机安全
Computer Security Incident	计算机安全事件
Computer Security Incident Response Team (CSIRT)	计算机安全事件响应组
Computer Security Object (CSO)	计算机安全对象
Computer Security Objects Register	计算机安全对象注册
Computer Security Subsystem	计算机安全性子系统
Computer Virus	计算机病毒
Computing Device	计算装置
Computing Environment	计算环境
Computing Individual Bits	计算单个比特
COMSEC	Communications Security 通信安全
COMSEC Account	通信安全账户
COMSEC Account Audit	通信安全账户审核
COMSEC Aid	通信安全援助
COMSEC Assembly	通信安全组件
COMSEC Boundary	通信安全边界
COMSEC Chip Set	通信安全芯片组

COMSEC Control Program	通信安全控制程序
COMSEC Custodian	通信安全托管人
COMSEC Demilitarization	通信安全设备脱密处理
COMSEC Element	通信安全部件
COMSEC End-Item	通信安全成品，通信安全最终产品
COMSEC Equipment	通信安全设备
COMSEC Facility	通信安全设施
COMSEC Incident	通信安全事件
COMSEC Insecurity	通信安全隐患
COMSEC Manager	通信安全经理
COMSEC Material	通信安全器材
COMSEC Material Control System (CMCS)	通信安全器材控制系统
COMSEC Modification	通信安全修正，通信安全修改
COMSEC Module	通信安全模块，通信安全组件
COMSEC Monitoring	通信安全监控
COMSEC Profile	通信安全措施简要介绍，通信安全概要
COMSEC Survey	通信安全概况
COMSEC System Data	通信安全系统数据
COMSEC Training	通信安全培训
Concealment	隐藏，隐藏性
Concept of Operations (CONOP)	操作概念
Conceptual Approach	概念研究
Concrete Intractability Assumption	具体难解的假设
Concrete Security	具体安全性
Concurrent Composition	并发复合
Concurrent Security	并发安全性

Concurrent Setting	并发设置
Concurrent Zero Knowledge	并发零知识
Concurrent Zero Knowledge Protocol	并发零知识协议
Condition Masking	条件掩饰，条件加罩
Conditional Correlation Attack	条件相关攻击
Conditional Entropy	条件熵
Conference Key	会话密钥
Conference Keying	会话密钥建立
Confidentiality	机密，机密性
Confidentiality, Integrity and Availability	机密性、完整性和可靠性
Configuration Control	配置控制
Configuration Control Board (CCB)	配置控制委员会
Confinement Channel	隐蔽信道
Confirmer Signature	证实者签名
Confirming Operation	确认操作
Confusion	混乱，混乱性
Confusion Block Cipher	混淆分组密码
Congruence	同余式
Congruence Class	同余类
Congruent	同余的
Conjecture	猜想
Conjugacy Class	共轭类
Conjugate	共轭的，结合的，轭合物
Conjunctive Search	连接搜索
Connection Polynomial	连接多项式
Consecutive Run	连续运行，游程

Consistent Sampling	持续抽样
Constant	常数，常量
Constant Depth	固定深度
Constant Rate Tampering	恒率篡改
Constant Round	常数轮
Constant Round Protocol	常数轮协议
Constant-Size Public Key	具有恒定大小的公钥
Constant-Time Scalar Multiplication	固定时间标量乘法
Constructible Regular Ngon	构造正则多边形
Constructability (Euclidean)	构造性（欧几里得）
Consumable Credential	消费凭证
Container	封装文件，容器文件，包
Containing	包容
Contamination	污染，混杂
Content Filtering	内容过滤
Content of a Polynomial	多项式的容度
Content Protection for Recordable Media	录制媒介内容保护
Content Scrambling System	内容加扰系统
Contingency Key	应急密钥
Contingency Plan	应急计划
Continual Auxiliary Leakage	持续辅助泄漏
Continual Leakage	持续泄漏
Continued Fraction	连分数
Continued Fraction Method	连续分数法
Continued Fraction Recursion Formula	连分数递归公式

Continuity of Government (COG)	政府延续性，政府持续运转
Continuity of Operations Plan (COOP)	运行规划连续性
Continuous Monitoring	连续监控
Contract Signing	合同签署，合约签署
Contrast	对比度
Contrived	虚假的
Control	控件
Control Information	控制信息
Control Not Gate	控制非门
Control Vector	控制向量
Controlled Access Area	受控访问区域
Controlled Access Protection	受控访问保护
Controlled Area	控制区
Controlled Cryptographic Item (CCI)	受控密码产品
Controlled Cryptographic Item (CCI) Assembly	受控密码产品组件
Controlled Cryptographic Item (CCI) Component	受控密码产品部件
Controlled Cryptographic Item (CCI) Equipment	受控密码产品设备
Controlled Facility	受控设施
Controlled Interface	控制界面，控制接口
Controlled Space	受控空间
Controlled Unclassified Information (CUI)	受控非加密信息
Controlled-Malleable	可控延展的

Controlling Authority	监管部门
Conventional Cryptosystem	常用密码系统，传统加密体制
Convergent	收敛
Convergent Encryption	收敛加密
Conversation	对话，会话
Convertible Undeniable Signature	可转换不可否认签名
Convex Geometry	凸几何
Convex Set	凸集
COOP	Continuity of Operation Plan 运行规划连续性
Cooperative Key Generation	合作密钥生成
Cooperative Remote Rekeying	合作远程密钥更新
Coppersmith Theorem Attack	Coppersmith 定理攻击
Copy Generation Control	拷贝生成控制
Copy Marking	复制标记
Copy Protection	复制保护
Copy Right Protection	版权保护
Core Messaging Platform	核心报文处理平台
Core Round	核心轮
Corporate Message Recovery	企业信息恢复
Correct Opening	正确的公开问题
Correcting-Block Attack	修改消息块攻击
Correctness Proof	正确性证明
Correlated Equilibria Mediator	相关平衡中介者
Correlation Immunity Order	相关免疫阶
Correlation Power Analysis	相关能量分析
Correlation-Immune and Resilient Boolean Function	相关免疫及弹性布尔函数
Correspondence	对应

Coset	陪集
Coset Space	陪集空间
Counter Collision	抗碰撞
Counter Mode	计数器模式
Counter with Cipher Block Chaining-Message Authentication Code	计数器及密码分组链接消息认证码
Counter Example	反例
Counterfeiting	伪造
Counterintuitive	违反直觉的
Countermeasure	对抗
Counting	计数
Cover	覆盖
Cover and Decomposition Attack	覆盖和分解攻击
Cover and Decomposition Index Calculus	覆盖和分解指标计算
Cover Signal	载体信号
Coverage	覆盖范围
Cover-Coding	隐藏编码
Covert Channel	隐蔽信道
Covert Channel Analysis	隐蔽信道分析
Covert Security	隐蔽安全模型
Covert Storage Channel	隐蔽存储信道
Covert Testing	隐蔽检测
Covert Timing Channel	隐蔽时间信道
Covertext	伪装文本，掩饰文本
CPRM	Content Protectionfor Recordable Media 多媒体资料内容保护

CR	Composite Residuosity 复合剩余
Cramer-Shoup Public Key Scheme	Cramer-Shoup 公钥方案
Credential	信任证，凭证，凭据
Credential Service Provider (CSP)	凭据服务提供商
CRHF	Collision Resistant Hash Function 抗碰撞哈希函数
Crisis	危机
Crisis Management	危机管理
Crisis Management Plan	危机管理计划
Critical Infrastructure	关键基础设施
Critical Security Parameter (CSP)	关键安全参数
Criticality	关键度，关键性
Criticality Level	临界水平，风险程度
CRL (CRLs)	Certificate Revocation List 证书吊销列表
Cross Certificate	交叉认证，全跨凭证
Cross Correlation	互关联（互相关）
Cross Site Scripting (XSS)	跨站脚本，交叉位置脚本，跨站式注入
Cross-Domain Capability	跨域功能
Cross-Domain Solution (CDS)	跨域解决方案
Crossing Step	交叉步
Crowd-Blending Privacy	群体混合隐私
Crowds	Crowds 系统
CRT	Chinese Remainder Theorem 中国剩余定理，孙子剩余定理
Cryptanalysis	密码分析

Cryptanalytic	密码分析的
Crypto Machine	密码机
Crypto Officer	密码主管
Cryptographer	密码学家
Cryptographic	密码的，加密的
Cryptographic Alarm	密码警报
Cryptographic Algorithm	密码算法，加密算法
Cryptographic Ancillary Equipment	加密辅助设备
Cryptographic Binding	密码绑定
Cryptographic Boundary	密码界限
Cryptographic Component	密码组件
Cryptographic Equipment	密码设备，加密设备
Cryptographic Hash Function	密码哈希函数，密码散列函数
Cryptographic Hashing	密码哈希
Cryptographic Ignition Key (CIK)	密码键
Cryptographic Implementation	密码方案，密码实现
Cryptographic Initialization	密码初始化
Cryptographic Key	密钥
Cryptographic Logic	密码逻辑，加密逻辑
Cryptographic Material (Slang Crypto)	加密材料
Cryptographic Message Syntax	密码消息语法，密码信息语法
Cryptographic Module	密码模块，密码模件
Cryptographic Module Security Policy	密码模块安全策略
Cryptographic Module Validation Program (CMVP)	密码模块验证体系，密码模块验证流程

Cryptographic Net 密码网
Cryptographic Period 密码周期
Cryptographic Primitive 密码原语，密码基本组件
Cryptographic Product 密码产品
Cryptographic Protocol 密码协议，安全协议
Cryptographic Randomization 密码随机化
Cryptographic Scheme 密码方案
Cryptographic Security 密码安全
Cryptographic Strength 密码强度
Cryptographic Synchronization 密码同步
Cryptographic System 密码系统
Cryptographic System Analysis 密码系统分析
Cryptographic System Evaluation 密码系统评估
Cryptographic System Review 密码系统审查
Cryptographic System Survey 密码系统调查
Cryptographic Token 密码令牌
Cryptology 密码学，密码术
Cryptosystem 密码系统
CRYPTREC Cryptography Research and Evaluation Committees 日本政府成立的“密码研究与评估委员会”
Crystallographic Group 晶体群
CS-Lite Cramer-Shoup 简化系统
CSP Critical Security Parameters 关键安全参数
CSS Content Scrambling System 内容加扰系统，内容加密系统

CTCPEC	Canadian Trusted Computer Product Evaluation Criteria 加拿大可信计算机产品评估标准
CTR	Counter 对抗
Cube Number	立方数
Cubic and Quartic	三次和四次的
Cubic Residue	三次剩余
Cue	术语代码信息
Customer Acquirer	消费者支付服务提供者
Cut-and-Choose Protocol	分割和选择协议
Cut-Query	切入查询
CVE	Common Vulnerabilities and Exposures 通用漏洞列表，通用漏洞披露
CVP	Closest Vector Problem 最近向量问题
CWC	Carter-Wegman + CTR mode，CWC 模式
Cyber Attack	网络攻击
Cyber Incident	网络事件
Cyber Infrastructure	网络基础设施
Cybersecurity	网络安全
Cyberspace	网络空间
Cycle	周期
Cyclic	周期的，循环的，轮转的
Cyclic Code	循环码
Cyclic Group	循环群
Cyclic Reed-Muller Code	循环 Reed-Muller 代码
Cyclical Redundancy Check (CRC)	循环冗余校验
Cycling Attack Against RSA	对 RSA 的循环攻击
Cyclotomic	分圆的

Cyclotomic Coset	分圆陪集
Cyclotomic Field	分圆域
Cyclotomy Method	分圆法
Cyrillic Alphabet	西里尔字母

D

Damage Assessment	损害评估
Data	数据
Data Aggregation	数据融合
Data Asset	数据资产
Data Authentication	数据认证
Data Block	数据分组
Data Center Recovery	数据中心恢复
Data Clustering	数据聚类
Data Complexity	数据复杂度
Data Element	数据元
Data Encapsulation Mechanism	数据封装机制
Data Encryption Algorithm (DEA)	数据加密算法
Data Encryption Standard (DES)	数据加密标准
Data Flow Control	数据流控制
Data Integrity	数据完整性
Data Loss Prevention (DLP)	数据丢失防护
Data Key	数据密钥
Data Loss	数据丢失
Data Masking	数据屏蔽
Data Origin Authentication	数据来源认证
Data Remanence	数据残留
Data Seal	数据密封
Data Security	数据安全

Data Transfer Device (DTD)	数据传输设备
Davies Attack	Davies 攻击
DC Network	直流网络
DCRA	Decisional Composite Residuosity Assumption 判定性复合剩余假设
DDA	Dynamic Data Authentication 动态数据认证
DDH	Decisional Diffie-Hellman (DDH) Assumption 判定性 Diffie-Hellman 假设
De Bruijn Graph	De Bruijn 图形
De Bruijn Sequence	De Bruijn 序列
De Viaris Attack	De Viaris 攻击
Decapsulate	解封，解开
Deception	欺诈
Decertification	取消认可
Decimation	抽取
Decipher	解密
Decision Function	决策函数
Decision Linear (DLIN) Assumption	决策线性假设
Decision Linear Problem	决策线性问题
Decisional Composite Residuosity Assumption	判定性复合剩余假设
Decisional Diffie-Hellman Problem	判定性 Diffie-Hellman 问题
Decisional Linear (DLIN) Problem	判定线性问题
Decisional Linear Assumption	判定线性假设
Decision-Making Module	决策制定模块
Declaration Fee	报关费

Decode	解码
Decommitment	解除承诺
Decomposing Point of the Curve	曲线分解点
Decomposition Into	分解成
Decomposition-Based Index Calculus	基于分解的指标计算法
Decorrelation	去相关
Decrypt	解密，译码（动词）
Decryption	解密，译码
Decryption Algorithm	解密算法
Decryption Exponent	解密指数
Decryption Query	解密查询
Decryption Steps	解密步骤
Dedekind Independence Theorem	Dedekind 独立性定理
Dedicated Line	专用线路
Dedicated Mode	专用模式
Deduplication	重复数据删除
Deep Crack	深度裂缝
Default Classification	默认分类
Defense-in-Breadth	拓宽防御
Defense-in-Depth	纵深防御
Deficient Number	不足数
Defined by a Linear Transform Ion	通过一个线性变换离子被定义
Definitely Composite	绝对合成
Degauss	消磁
Degrade	分解

Degree	度，次
Degree of a Polynomial	多项式次数
Delayed Measurement Technique	延时测量技术
Delegated Development Program	委托发展计划
Delegated Path Discovery	委托路径查询
Delegated Path Validation	委托路径确认
Delegation	委托
Della Porta's Maxim	德拉波普准则
DEM	Data Encapsulation Mechanism 数据封装机制
DEMA	Differential Electromagnetic Analysis 差分电磁分析
Demilitarized Zone（DMZ）	（无警戒区）隔离区
Denary Alphabet	十进制字母表示
Deniable Encryption	可否认加密
Denial of Service（DOS）	拒绝服务
Denote	表示
Density	密度
Density Matrix	密度矩阵
Dependency	关联性，依赖关系
Deprovisioning	断开连接，解除配置
Depth	深度
Derandomization	去随机
Derangement	错排数
Derivation	推导，导出，求导，导数
Derivative	派生的，导数
Derived Key	派生密钥
Derived Test Requirement	提取测试需求

DES	Data Encryption Standard 数据加密标准
Descent	降阶法
Descriptive Top-Level Specification（DTLS）	陈述式顶层规格，描述性的顶级规格
Design Rationale	设计原理
Designated Approval Authority（DAA）	指定的审批机构
Designated Combiner	指定组合器
Designated Confirmer Signature	指定证实者签名
DES-MAC	基于 DES 的 MAC 算法
Desmedt-Vandewalle-Govaerts Knapsack	Desmedt-Vandewalle-Govaerts 背包问题
DES-X	扩展数据加密标准
Determinant	决定因素，行列式
Deterministic	确定性的
Deterministic and Efficiently Searchable IBE Scheme	确定有效的基于身份加密方案
Deterministic Ciphertext	确定性密文
Deterministic Encryption	确定性加密
Deterministic Finite Automata	确定性有限自动机
Deterministic Function	确定性函数
Deterministic Public-Key Encryption	确定性公钥加密
Deterministic Random Bit Generator（DRBG）	确定性随机数发生器
Deterministic Random Bit Generator（DRBG）Mechanism	确定性随机数发生器机制
Device Distribution Profile	装置分布配置文件

Device Registration Manager	设备注册经理
DFA	Differential Fault Analysis 差分故障分析
DHP	Diffie-Hellman 问题（DHP = Diffie-Hellman Problem）
Diagonal	对角线的，斜的
Diagram	图表
Dial Back	回拨
Dial Backup	拨号备份
Dial-Up Line	拨号线路
Dictionary	代码词典
Dictionary Attack	字典式攻击，词典式攻击
Difference Distribution Table	差分分布表
Difference of Successive Convergent Theorem	相邻收敛之差定理
Difference Set	差集
Differential Analysis	差分分析
Differential Attack	差分攻击
Differential Characteristic	差分特征
Differential Cryptanalysis	差分分析
Differential Distribution Table (DDT)	差分分布表，微分分布盒
Differential Electromagnetic Analysis	差分电磁分析
Differential Fault Analysis	差分故障分析
Differential Meet-in-the-Middle	差分中间相遇
Differential Membership Test	差分资格测试
Differential Power Analysis (DPA)	差分能量分析

Differential Privacy	差分隐私性
Differential Property	差分特性
Differential-Linear Attack	差分线性攻击
Diffie-Hellman Key Agreement	Diffie-Hellman 密钥协商
Diffie-Hellman Problem	Diffie-Hellman 问题
Diffusion	扩散
Diffusion Block Cipher	扩散分组密码
Digital Certificate	数字证书
Digital Evidence	数字证据
Digital Forensics	数字取证
Digital Identity	数字身份
Digital Locking System	数字锁定系统
Digital Millennium Copyright Act	数字千年版权法案
Digital Rights Management System	数字版权管理系统
Digital Signature	数字签名
Digital Signature Algorithm	数字签名算法
Digital Signature Guideline	数字签名指南
Digital Signature Scheme	数字签名方案
Digital Signature Standard	数字签名标准
Digital Steganography	数字密写，信息隐藏技术
Digital Versatile Disk	数字通用光盘
Digital Video Disk	数码光碟
Digital Watermarking	数字水印
Digraphic Substitution	有向图替换
Dihedral	二面角
Diophantine	丢番图的
Diophantine Approximation	丢番图逼近

Diophantine Approximation Theorem	丢番图逼近定理
Diophantine Equation	丢番图方程
Diophantus of Alexandria	丢番图
Direct Cross-Certification	直接交叉认证
Direct Ingredient	直接因素
Direct Inversion	直接反演
Direct Payment Scheme	直接支付方案
Direct Product	直积
Direct Sum	直和
Direct Sum of Modules	模的直和
Dirichlet's Diophantine Approximation Theorem	狄利克雷丢番图逼近定理
Dirichlet's Theorem on Primes in Arithmetic Progressions	算术级数的狄利克雷素数定理
Disaster Prevention	灾难防治措施
Disaster Recovery	灾难恢复
Disaster Recovery Plan (DRP)	灾难恢复计划，灾后恢复计划
Disaster Recovery Planning	灾难恢复设计
Disconnection	截断，断开
Discrete	离散的
Discrete Fourier Transform	离散傅里叶变换
Discrete Logarithm	离散对数
Discrete Logarithm Problem	离散对数问题
Discrete-Log	离散对数
Discretionary Access Control	自主访问控制
Discriminant	判别式

Dishonest Majority	不诚实多数
Disjoint	不相交
Disk Imaging	磁盘映像
Disqualify	使失去资格
Disquisitiones Arithmeticae	算术研究
Disruption	破坏
Dissection of Composite Problem	复合问题的有效分离
Distill	提取
Distinguished Name（DN）	标识名称
Distinguished Point	可辨识点
Distinguisher	区分器
Distinguishing Algorithm	区分算法
Distinguishing Attack	区分攻击
Distinguishing Identifier	可区分的标识
Distributed Denial of Service（DDOS）	分布式拒绝服务
Distributed DOS Attack	分布式拒绝服务攻击
Distributed Key Generation	分布式密钥生成
Distributed Processing	分布处理
Distributive	分布的
Distributive Law	分配律
Distributivity	分配性
Divide-and-Conquer Attack	分割和统治攻击
Divisibility	整除性
Division	除法
Division Intractable	除困难性
Divisor	因子，因数，除子

Dixon's Random Squares Method	（连分数分解法）Dixon 随机平方算法
DLP	Distributed Logic Programming 分散式逻辑程式设计
DMCA	Digital Millennium Copyright Act 数字千年版权法案
DMZ	Demilitarized Zone 非军事区，隔离区
DNS	Domain Naming Service 域名服务
Document Imaging	文档成像（扫描印刷文档转换为数字图像过程）
Domain	定义域，整环
Domain Naming Service（DNS）	域名服务
Domain Parameter	定义域参数
DOS	Denial of Service 拒绝服务
DOS Robustness	DOS 强健性
Double Block Length Hashing	双分组长度哈希
Double Key	双重密钥
Double-and-Add	加倍和加算法
Double-Branch Hash Function	双分支哈希函数
Double-DES	双重 DES
Double Precision IEEE Standard	双精度 IEEE 的标准，IEEE 电气与电子工程师协会（Institute of Electrical and Electronic Engineers）
Double Sharing	双倍共享
DPA	Differential Power Analysis 差分能量分析
DPD	Delegated Path Discovery 委托路径查询
DPV	Delegated Path Validation 委托路径确认
DRM	Digital Rights Management 数字版权管理
DRMS	Digital Rights Management System 数字版权管理系统

Drop Accountability	丢弃责任
DRP	Disaster Recovery Plan 灾难恢复规划
DSA	Digital Signature Algorithm 数字签名算法
DSG	Digital Signature Guideline 数字签名指南
DSS	Digital Signature Standard 数字签名标准
Dual （or Complementary）	对偶的，补充的
Dual Code	对偶码
Dual Form Signature	对偶形式签名
Dual Pairing Vector Spaces （DPVS）	偶对向量空间
Dual Projective Hashing	对偶投影哈希
Dual System Encryption	双系统加密
Dual-System IBE	双系统 IBE
Dual-Use Certificate	两用证书
Duplex Construction	双工结构
Duplicate Digital Evidence	复制数字证据
Duration	持续时间
Dynamic Adversary	动态敌手，动态对手
Dynamic Attribute	动态属性
Dynamic Authentication	动态认证
Dynamic Credential	动态证据
Dynamic Data Authentication	动态数据认证
Dynamic Group Signature Scheme	动态群签字方案
Dynamic Storage	动态存储
Dynamic Subsystem	动态子系统
Dynamic Traitor Tracing	动态叛徒追踪

E

E0（Bluetooth）	E0 算法（蓝牙）
EAL	Evaluation Assurance Level 信息安全产品测评认证级别
Eavesdropper	窃听者
Eavesdropping Attack	窃听攻击
EAX	Electronic Automatic Exchange 电子自动交换机
ECB	Electronic Components Board 电子部件局
ECC	Error Correction Code 纠错码，Elliptic Curve Cryptography 椭圆曲线密码学
ECC Challenge	Error Correction Code Challenges 纠错码挑战
ECDLP	Elliptic Curve Discrete Logarithm Problem 椭圆曲线离散对数问题
ECDSA	Elliptic Curve Digital Signature Algorithm 椭圆曲线数字签名算法
ECIES	Elliptic Curve Integrated Encryption Scheme 椭圆曲线集成加密机制
ECMS	Electronic Coding Machine System 电子编码机系统
ECPP	Elliptic Curve Primality Proving 椭圆曲线素性证明
EDI	Electronic Data Interchange 电子数据交换
Egress Filtering	外出过滤，出口过滤
Einstein-Podolsky-Rosen（EPR）Pair	EPR 对（EPR＝爱因斯坦、波多尔斯基和罗森）

Electromagnetic Attack	电磁攻击
Electromagnetic Pulse	电磁脉冲
Electronic Authentication (E-Authentication)	电子认证
Electronic Business (E-Business)	电子商务
Electronic Cash	电子现金
Electronic Cheque	电子支票
Electronic Codebook Mode (ECB)	电子电报密码本模式，电码本模式
Electronic Coin	电子货币
Electronic Commerce	电子商务
Electronic Copyright Management System	电子版权管理系统
Electronic Credential	电子凭证
Electronic Data Interchange (EDI)	电子数据交换
Electronic Evidence	电子取证
Electronic Frontier Foundation	电子前线基金会，电子前沿基金会
Electronic Funds Transfer	电子资金转账
Electronic Key Entry	电子密钥登录
Electronic Key Management System (EKMS)	电子密钥管理系统
Electronic Lock	电子锁
Electronic Messaging Service	电子报文服务
Electronic Negotiable Instrument	电子流通票据，电子票据
Electronic Noise Source	电子干扰源，电子噪声源

Electronic Payment	电子支付
Electronic Postage	电子邮费
Electronic Purse	电子财力，电子钱包
Electronic Signature	电子签名
Electronic Vaulting	电子跨越，电子传送
Electronic Voting Scheme	电子投票方案
Electronic Wallet	电子钱包
Electronically Generated Key	自动生成密钥
Element	原理，元件
Elements of Euclid	欧几里得的《几何原本》
Element-wise Exponentiation	逐元素指数化
Elgamal Cryptosystem	阿尔加莫密码体制
Elgamal Digital Signature Scheme	阿尔加莫数字签名（机制）方案
Elgamal Encryption	阿尔加莫加密
Elgamal Public Key Encryption	阿尔加莫公钥加密
Ellipse	椭圆
Elliptic Curve Cryptography	椭圆曲线密码学
Elliptic Curve Discrete Logarithm Problem (ECDLP)	椭圆曲线离散对数问题
Elliptic Curve Factorization	椭圆曲线因子分解
Elliptic Curve Integrated Encryption	椭圆曲线综合加密
Elliptic Curve Key	椭圆曲线密钥
Elliptic Curve Key Agreement Scheme	椭圆曲线密钥协商机制
Elliptic Curve Method (ECM)	椭圆曲线方法
Elliptic Curve Method for Factoring	椭圆曲线因子分解方法

Elliptic Curve Point Multiplication Using Halving	使用二等分的椭圆曲线要点乘法
Elliptic Curve	椭圆曲线
Elliptic Curve for Primality	椭圆曲线素性检测
Elliptic Curve Primality Proving Algorithm	椭圆曲线素性证明算法
Elliptic Curve Public Key	椭圆曲线公钥
Elliptic Curve Signature Scheme	椭圆曲线签名方案
EMA	Electromagnetic Accelerometer 电磁加速计
EMAC	Ethernet Media Access Control 以太网媒体访问控制器
Emanation Security (EMSEC)	发射安全
Embedded Computer	嵌入式计算机
Embedded Cryptographic System	嵌入式密码系统
Embedded Cryptography	嵌入式密码（使用法）
Emergency	紧急事件
Emergency Preparedness	应急准备
Emergency Response Procedure	应急反应程序
EMP	Electromagnetic Pulse 电磁脉冲
Empirical	经验的
Empirically Verifiable Assumption	经验性验证假设
EMV	Electromagnetic Volume 电磁电容
Encapsulating Security Payload	封装安全性有效载荷

Encipher	加密（动词）
Enciphering	加密
Enciphering Scheme	加密方案
Enclave	飞地，被包围的领土，指定位置空间
Enclave Boundary	区域边界
Encode	编码（动词）
Encrypt	加密（动词）
Encrypt Copyrighted Content	把有版权的内容加密
Encrypt-and-MAC	加密和消息认证码
Encrypted Key	密钥，被加密的密钥
Encrypted Network	加密网络
Encrypted Vote	加密的选票
Encryption	加密，加密术
Encryption Algorithm	加密算法
Encryption Certificate	加密证书
Encryption Exponent	加密指数
Encryption Key	加密密钥
Encryption Rule	加密规则
Encryption Scheme	加密方案
Encryption Step	加密步骤
Encrypt-then-MAC	加密然后消息认证码
End Cryptographic Unit (ECU)	端加密单元
End Entity	终端实体
End-Item Accounting	端项审核
End-of-Proof-Marker	证毕标志
Endomorphic Cryptosystem	自同态密码系统
Endomorphism	自同态
Endomorphism of a Module	模的自同态

Endomorphism of an Abelian Group	阿贝尔群的自同态
End-to-End Encryption	端到端加密
End-to-End Security	端到端安全
Enforcement	强制执行，强制
Enigma	英格玛密码机
Enrollment Manager	注册经理人，注册管理器
Entangled State	纠缠态
Enterprise	企业
Enterprise Architecture (EA)	企业体系
Enterprise Risk Management	企业风险管理
Enterprise Service	企业服务
Enterprise Vulnerability Management System (EVMS)	启业漏洞管理系统
Entitlements Management	权益管理
Entity	实体
Entity Authentication	实体鉴别
Entrapment	圈套，陷阱
Entropic Uncertainty Relation	熵的不确定关系
Entropy	熵
Envelope	信封，包膜
Envelope MAC	封装 MAC
Environment of Operation	操作环境
Environmental Disaster	环境灾难
Environmental Threat	环境威胁
EPC	Extended Parity Checking 扩展的奇偶核对
Ephemeral	短暂的
Ephemeral Diffie-Hellman	临时 Diffie-Hellman
Ephemeral Key	临时密钥

Equilibrium Notion	平衡性概念
Equivalence	等价
Equivalence Relation Defined by	等价关系被……定义
Equivalent	相等的，相当的，等效的，等价的，等积的
Equivalent Group Action	等价群作用
Equivocation	条件信息量总平均值
Erasure	抹除，擦除
Erasure-Free	免擦除
Error Detection Code	纠错码
Escrow	第三方支付，托管（由第三者保存附带条件委付盖印的契约）
ESP	Electronic Stability Program 电子稳定程序
Essential Records	必要文档
Ethernet	以太网
ETM	Embedded Trace Macrocell 嵌入式跟踪宏单元
Euclid	欧几里得
Euclidean Algorithm	欧几里德算法
EU-CMA	欧盟计量认证
Euler Liar	欧拉撒谎者
Euler Pseudo-prime	欧拉伪素数
Euler's Constant	欧拉常数
Euler's Criterion	欧拉准则
Euler's Formula	欧拉公式
Euler's Identity	欧拉恒等式
Euler's Perfect Number Theorem	欧拉完全数定理

Euler's Phi Function	欧拉 Phi 函数
Euler's Theorem	欧拉原理
Euler's Totient Function	欧拉函数
Evaluation Assurance Level (EAL)	评估保证级别
Evaluation Key	求值密钥
Evaluation of Policy	评估政策
Evaluation Products List (EPL)	评估产品列表
Even and Odd	偶数和奇数
Even Number	偶数
Even-Mansour Construction	Even-Mansour 结构
Even-Mansour Scheme	Even-Mansour 方案（EM 方案）
Event	项目，事件
EVMS	Enterprise Vulnerability Management System 企业漏洞管理系统
E-Voting Scheme	电子投票方案
Exact Identification	精确鉴别
Excluded Subtree	被排除的子树
Exculpability Scheme	防陷害性方案
Exculpatory Evidence	辩护证据
Executive Agency	执行机构
Exercise Key	运行密钥
Exhaustive Key Search	穷举密钥搜索，彻底密钥搜索
Exhaustive Search	穷举搜索
Existential Forgery	存在性伪造
Existential Unforgeability	存在性不可伪造
Expansion	扩张
Expected Differential Probability	预期差分概率

Expected Output	预期（结果）的输出
Explicit Policy Indicator	明确的政策指示
Exploit Code	漏洞检测代码
Exploitable Channel	可利用信道
Exponential	指数的
Exponential Generating Function	指数生成函数
Exponential Growth	指数增长
Exponential Security	指数的安全性
Exponential Time	指数时间
Exponentiation	求幂运算
Extended Euclidean Algorithm	扩展的欧几里德算法
Extended MD4	扩展的 MD4 算法
Extensible Configuration Checklist Description Format (XCCDF)	可扩展配置对照表格式说明
Extension Degree	扩展次数
Extension Field	扩张域
Extension Field Operation	扩展域运算
Exterior	外部
External Collision	外部撞击
External Information System (or Component)	外部信息系统（或成分，部件）
External Information System Service	外部信息系统服务
External Information System Service Provider	外部信息系统服务供应商
External Network	外部网络

External Security Testing	外部安全性测试
Extra Expense Coverage	额外费用保险
Extract Witness	提取证据
Extraction Procedure	抽取程序
Extraction Resistance	提取抵抗
Extractor	提取器
Extranet	外联网
Extremal Graph	极值图

F

Factor	因子
Factor Basis	因子基
Factorial	因子的，阶乘的；阶乘
Factoring	因式分解
Factoring Circuit	因式分解电路
Factoring Problem	因式分解问题
Factorization	因子分解
Factorization Algorithm	分解算法
Factorization Method	分解法
Fail Safe	故障保护，失效安全
Fail Soft	故障弱化
Failover	失效备援
Fail-Stop Signature	失败停止签名，故障停止签名
Failure Access	故障访问，失效访问
Failure Control	故障控制
Failure Probability	失败概率
Fair Blind Signature	公平盲签名
Fair Coin-Tossing Problem	公平抛硬币问题
Fair Computation	公平计算
Fair Exchange	公平交换
Fair Protocol	公平协议
Fair Sampling Problem	公平抽样问题
Fairness	公平
False Acceptance	误接收
False Acceptance Rate（FAR）	误接收率

False Negatives	漏报率
False Positive	假阳性
False Reject Error	虚假拒绝错误，虚假驳回错误
False Rejection	误拒绝
False Rejection Rate (FRR)	误拒绝率
Families of Elliptic Curves	椭圆曲线族
Fast Algebraic Attack	快速代数攻击
Fast Correlation Attack	快捷关联攻击
Fast Data Encipherment Algorithm	快捷数据加密算法
Fast Endomorphism	快速自同态
Fast Fourier Transform (FFT)	快速傅里叶变换
Fault Attack	故障攻击
Fault Generation	故障生成
Faulty Share	缺省份额
Feature Extraction Module	特征抽取模块
Federal Agency	联邦机构
Federal Bridge Certification Authority (FBCA)	联邦桥式认证机构
Federal Bridge Certification Authority Membrane	联邦桥式认证机构膜
Federal Bridge Certification Authority Operational Authority	联邦桥式认证机构操作方
Federal Enterprise Architecture	联邦企业架构
Federal Information Processing	联邦信息处理
Federal Information Processing Standard (FIPS)	联邦信息处理标准

Federal Information Security Management Act（FISMA）	联邦信息安全管理法案
Federal Information System	联邦信息系统
Federal Information Systems Security Educators' Association（FISSEA）	联邦信息系统安全教育者联合会
Federal Public Key Infrastructure Policy Authority（FPKIPA）	联邦公共密钥基础设施局
Feedback Bit	反馈比特
Feedback Coefficient	反馈系数
Feedback Function/Polynomial	反馈函数/多项式
Feedback Shift Register	反馈移位寄存器
Feige-Fiat-Shamir Signature Scheme	法伊格、菲亚特、沙米尔签名方案
Feistel Cipher	费斯托密码
Feistel Network	费斯托网络
Fermat Liar	费马撒谎者
Fermat Primality Test	费马素性测试
Fermat Prime	费马素数
Fermat's Last Theorem	费马大定理
Fermat's Little Theorem	费马小定理
Fermat's Method of Descent	费马降阶法
Fiat-Naor Construction	菲亚特瑙尔结构
Fiat-Shamir Identification Protocol and Feige Fiat-Shamir Signature Scheme	菲亚特沙米尔识别协议和法伊格、菲亚特、沙米尔签名方案
Fiat-Shamir Transformation	菲亚特沙米尔转换

FIB	Focused Ion Beam 聚焦离子束
Fibonacci Generating Function Formula	斐波那契生成函数公式
Fibonacci Sequence	斐波那契数列
Field	域
Field Inversion	域的逆（运算）
Field Polynomial	域多项式
FIFO	First In First Out 先入先出缓冲器
File Encryption	文件加密
File Name Anomaly	文件名称异常
File Protection	文件保护
File Security	文件安全
File Server	文件服务器
Fill Device	填充装置
Filter	滤波器
Filter Generator	过滤发生器
Filtering（Packets）	过滤（数据包）
Final Finished Message	最后完成的消息
Fine Grained	细粒度
Fingerprinting	指纹识别
Fingerprinting Code	指纹识别代码
Finite	有限的
Finite Fair Sampling Problem	有限公平抽样问题
Finite Field	有限域
Finitely Generated	有限生成的
Finitely Presented	有限表现，有限表示
FIPS	Federal Information Processing Standard 联邦信息处理标准
FIPS Pub	Federal Information Processing Standards Publications 联邦信息处理标准出版物

FIPS-Approved Security Method	联邦信息处理标准已批准安全方法
FIPS-Validated Cryptography	联邦信息处理标准已验证加密术
Firewall	防火墙
Firewall Control Proxy	防火墙控制代理
Firmware	固件
First and Second Isomorphism Theorems	第一和第二同构定理
Fischlin Scheme	Fischlin 方案
FISMA	Federal Information Security Management Act 联邦信息安全管理法案
Five-Card Trick	五张卡牌技巧
Fixed Argument Pairing Inversion Problem	固定参数对反演问题
Fixed COMSEC Facility	固定通信安全措施设施
Fixed Point Attack	不动点攻击
Fixed-Base Comb Method	固定基的梳算法
Fixed-Base Euclidean Method	固定基的欧几里德方法
Fixed-Base Exponentiation	固定基的幂
Fixed-Base Windowing Method	固定基的窗口方法
Fixed-Exponent Exponentiation	固定指数乘方
Flat Namespace	平面命名空间
Flaw	缺陷
Flaw Hypothesis Methodology	缺陷假说方法论
Flexible RSA Assumption	弹性 RSA 假设
Flip-Flop Metastability Source	触发器亚稳定性源
Floating-Point Arithmetic	浮点数运算

Flooding	泛洪
Flooding DOS Attack	泛洪 DOS 攻击
Flow	流量
Focused Ion Beam	聚焦离子束
Focused Testing	聚焦测试
Forensic Copy	司法复制
Forensic Specialist	法医学专家
Forensically Clean	法医清洁（在计算机领域指清除一切不需要的文件）
Forensic Imaging	取证扫描，取证成像
Forensics	取证，辩论术，法医学
Forger	伪造者
Forgery	伪造
Forgery Attack	伪造进攻
Forking Lemma	分叉引理
Form	形式，表格
Formal Access Approval	正式进入许可
Formal Development Methodology	规范化发展方法论
Formal Method	形式化方法
Formal Power Series	形式幂级数
Formal Proof	形式证明
Formal Security Policy	形式安全策略
Formalizing	形式化
Format-Preserving Encryption	格式保存加密
Formatting Function	格式化函数
Fortezza	堡垒
Forward Cipher	前向密码
Forward Mixing	前向混合

Forward Recovery	正向恢复
Forward Secrecy	前向保密
Four Color Problem	四色问题
Four Square Theorem	四平方定理
Four-Dimensional Decomposition	四维分解
Four-Message Argument	四消息参数
Fourier Argument	傅立叶参数
Fraction	分数
Fragmentation	存储残片，碎片
Frame	帧
Frame Counter	帧计数器
Frame Number	帧编号
Free Abelian	自由的和交换的
Free Objects	自由对象，自由个体
Free Text Search	自由文本搜索
Freedom Degree	自由度
Frequency Hopping	跳频
Frequency Matching	频率一致，频率匹配
Freshness	新鲜度
Frey Curve	弗雷曲线
Frobenius Generalization	弗罗贝尼乌斯扩展
Frobenius Map	弗罗贝尼乌斯映射
Frobenius' Theorem	弗罗贝尼乌斯定理
Frobenius-Grantham Primality Test	弗罗贝尼乌斯—格兰瑟姆素性测试
FSR	Feedback Shift Register 反馈移位寄存器
Fujiwara-Okamoto Transformation	藤原冈本转换

Full Disk Encryption (FDE)	全盘加密
Full Domain Hash Structure	全域散列结构
Full Key Size	全尺寸密钥长度
Full Maintenance	全面维修
Full Positive Difference Set	全正差集
Full-Domain Hash Method	全域哈希函数方法，全域散列法
Full-Knowledge Penetration Test	全知识渗透测试
Fully Homomorphic Encryption	完全同态加密
Fully Secure Cipher	完全加密算法
Function	函数
Function Field	函数域
Function Field Sieve	函数域筛
Functional Testing	功能测试
Functionality	泛函数，函数性
Fundamental Theorem	基本定理
Fundamental Theorem for Modules	模的基本定理
Fundamental Theorem for Monoids and Groups	幺半群和群的基本定理
Fundamental Theorem for Rings	环的基本定理
Fundamental Theorem of Algebra	代数基本定理
Fundamental Theorem of Arithmetic	算术基本定理
Fuzzy Extractor	模糊提取器

G

Galois Field	伽罗瓦域
Galois Group	伽罗瓦群
Galois Theory	伽罗瓦理论
Game	博弈
Game Theoretic Concept	博弈论概念
Game-Playing Technique	博弈技术
Game-Theoretic Consideration	博弈论的一些策略
Game-Theoretic Mechanism	博弈论机制
Gap	间隙
Gap Diffie-Hellman Assumption	间隙 Diffie-Hellman 假设
Gap Diffie-Hellman Group	间隙 Diffie-Hellman 群
Garbled Circuit	加密电路
Gate-by-Gate	逐门
Gateway	网关
Gauss' Lemma	高斯引理
Gauss Sum	高斯和
Gaussian Distribution	高斯分布
Gaussian Divisibility Lemma	高斯整除引理
Gaussian Integer	高斯整数
Gaussian Integer Method	高斯整数法
Gaussian Lattice Sampling	高斯格抽样
Gaussian Leftover Hash	高斯剩余散列
Gaussian Prime	高斯素数
Gaussian Prime Theorem	高斯素数定理

Gaussian Unit Theorem	高斯单位定理
Gauss's Criterion for Quadratic Residues	二次剩余的高斯判别法
GCD	Greatest Common Divisor 最大公因子
GCDH Assumption	GCDH 假设
Geffe Generator	Geffe 发生器
Gelfond-Schneider Theorem	盖尔范德和施耐德定理
General Adversary Model	一般对手模型
General Assumption	普遍假定
General Circuits Function Set	通用的电路函数集
General Construction	一般的构造
General Equation	一般方程
General Exponentiation	广义幂
General Functionality	一般功能
General Knapsack Scheme	广义背包方案
General Linear	一般线性
General Multicast Graph Setting	一般的多播图设置
General NFS	总体网络文件系统（NFS = Network File System）
General Purpose Algorithm	通用算法
General Purpose Primality Test	广义目标素性检测
General Support System	广义支撑集
Generality	普遍性
Generalized	广义的
Generalized Associativity	广义结合性，广义结合律
Generalized Feistel Structure	广义 Feistel 结构
Generalized Hurwitz Theorem	广义赫尔维茨定理

Generalized Inversion Attack	广义逆攻击
Generalized Mersenne Number	一般梅森数
Generalized Mersenne Prime	一般梅森质数
Generalized Subset Sum	广义子集和
Generated by a Subset	子集生成的
Generating Function	生成函数
Generator	发生器
Generator Matrix	生成矩阵
Generator Polynomial	生成多项式
Generic	通用类
Generic Algorithm	通用算法
Generic Amplification	通用扩展性
Generic Attack	普通攻击
Generic Attack Complexity	通用攻击复杂度
Generic Construction	一般性结构
Generic Cryptographic Primitive	一般密码基本组件
Generic Decoding Attack	普通解码攻击
Generic Discrete Logarithm Method	通用离散对数方法
Generic Distinguishing	一般区分分析
Generic Related-Key Attack	通用相关密钥攻击
Generic Security Analysis	通用的安全分析
Generic Transformation	类属转化
Gennaro-Halevi-Rabin Scheme	Gennaro-Halevi-Rabin 方案
Gentry's Fully Homomorphic Encryption	Gentry 完全同态加密

Genus 2 Based Cryptography	基于亏格为 2 的密码
Genus 2 Curve	亏格为 2 的曲线
Geometric Series	几何级数
Geometric Series Formula	几何级数公式
Geometry	几何学
Geometry of Numbers	数的几何
GHS Attack	GHS 攻击
Givierge's Maxim	Givierge 准则
Global Deduction	总体演绎
Global Information Grid (GIG)	全球信息网
Global Information Infrastructure (GII)	全球信息基础设施
Global Internet Routing System	全球互联网路由系统
Glue Logic Design	胶合逻辑设计
GLV Curve	GLV 曲线
GLV-Based Scalar Multiplication	基于 GLV 的标量乘法
GLV-GLS Method	GLV-GLS 方法
GMR Signature	GMR 签名
GNFS	General Number Field Sieve 一般数域筛法
GNU Privacy Guard	GNU 隐私卫士
GOC PKI	GOC 公钥基础设施
Golay Code	Golay 码
Gold Sequence	Gold 序列
Goldbach	哥德巴赫
Goldbach's Conjecture	哥德巴赫猜想
Golden Ratio	黄金比

Goldwasser-Micali Cryptosystem	Goldwasser-Micali 加密系统
Goldwasser-Micali Encryption Scheme	Goldwasser-Micali 加密机制
Golomb Ruler	Golomb 准则
Golomb's Randomness Postulates	Golomb 随机假设
Goppa Code	Goppa 码
Gost	Gost 密码算法
Government Data	政府数据
Government Entity	政府实体
Gröbner Basis	Gröbner 基
Graduated Security	分等级安全
Graham-Shamir Scheme	Graham-Shamir 方案
Graph Sparsification	图形稀疏化
Graphics Processing Units (GPU)	图形处理单元
Graph-Isomorphism	图同构
Gray Box Testing	灰盒测试
Greatest Common Divisor (GCD)	最大公约数
Grille	格栅
Groth-Sahai Proof	Groth-Sahai 证明
Groth-Sahai Proof System	Groth-Sahai 证明系统
Group Algebra	群代数
Group Authenticator	群认证器
Group Axioms	群组公理
Group Computational Diffie Hellman Assumption	群计算 Diffie Hellman 假设

Group Element	群元素
Group Key Agreement	群密钥协商
Group Key Distribution	群密钥分配
Group Manager	群组管理者
Group Name	群组名
Group of Transformation	变换群
Group of Units	单位群
Group Operation	群运算
Group Session Key	群组会话密钥
Group Signature	群签名
Group Size	群规模
Group to Group Commitment	群到群承诺
GSM	Global System for Mobile Communications 全球移动通信系统
Guard (System)	防护系统
Guess-and-Determine Attack	猜测决定攻击
Guessing Entropy	推测熵
Guessing Game	猜谜游戏
Guideline	指导方针
Guillou-Quisquater Signature Scheme	Guillou-Quisquater 签名方案

H

Hacker	黑客
Hadamard Gate	阿达马门
Hadamard Transform	阿达马变换
Hagelin	鲍里斯·哈格林（Boris Hagelin）设计的机械密码装置
Halftrace	半迹
Halving	二等分
Hamilton-Cayley-Frobemus Theorem	Hamilton-Cayley-Frobemus 定理
Hamiltonian Graph	汉密尔顿图
Hamming Distance	汉明间距
Hamming Metric Source	汉明度量源
Hamming Weight	汉明重量
Handshake	握手
Handshake Protocol	信号交换协议
Handshaking Procedure	握手程序
Hard Copy Key	硬拷贝密钥
Hard Core Bit	硬核比特
Hard Discrete-Logarithm Group	困难离散对数群
Hard Knapsack	硬背包
Hardcore Theorem	硬核定理
Hardening	硬化
Hardness Assumption	困难性假设
Hard-to-Compute Bits	难解比特

Hard-to-Invert Auxiliary Input	难逆辅助输入
Hard-to-Invert Leakage	难逆泄漏
Hardware	硬件
Hardware Security Module	硬件安全模块
Hardware Token	硬件令牌
Hardware-Assisted	硬件辅助的
Hardwired Key	电路密钥
Hash	哈希
Hash Function	哈希函数，散列函数
Hash Proof System	哈希证明系统
Hash Rate	哈希比率
Hash Total	哈希总和
Hash Value	哈希值
Hash Word	哈希字
Hash and Sign	哈希和签名
Hash-Based Message Authentication Code (HMAC)	基于哈希的信息认证码
Hashed	散列的
Hashing	哈希法，散列法
Hashing Key	哈希键
Hasse's Theorem	哈塞定理
Health Information Exchange (HIE)	健康信息交换
Hedged Scheme	对冲计划
Helios Cryptographic Voting System	Helios 加密投票系统
Helix	螺旋线
Hellmann's Time-memory Tradeoff	Hellmann 的内存时间折中

Hermite-Korkine-Zolotarev Lattice Reduction	HKZ 格规约
Hermite's Constant	埃尔米特常量
Hermitian	(矩阵) 厄密的
Heuristic Assumption	启发式假设
Heuristic Correction	启发式修正
HIBE	Hierarchical Identity-Based Encryption 基于分层的身份加密
Hidden Field	隐藏域
Hidden Subgroup Problem	隐藏子群问题
Hider	隐藏者
Hiding Assumption	隐藏假设
HIDS	Host Intrusion Detection System 主机型入侵检测系统
Hierarchical Namespace	分层命名空间
Hierarchically Ordered Random-Oracle	有序结构的随机预言
Hierarchy	阶层结构
High Assurance Guard (HAG)	高可信度防护
High Availability	高可用性
High Degree Polynomial Function	高次多项式函数
High Entropy Distribution	高熵分布
High Entropy Key	高熵密钥
High Impact	高冲力，高影响力
High Order DPA	高阶功耗攻击
High-Entropy	高熵
Higher Order Differential	高阶差分
Higher-Order Statistical Moment	高阶统计矩

High-Impact System	高冲力系统
High-Precision Floating Point Exponentiation	高精度浮点幂运算
Hilbert Irreducibility Theorem	希尔伯特不可约性定理
Hilbert Space	希尔伯特空间
Hilbert's Satz	希尔伯特命题
Hint	线索
HIPAA	Health Insurance Portability and Accountability Act 健康保险便利和责任法案
HIPS	Host Intrusion Prevention System 主机型入侵防护系统
Hirose's Scheme	Hirose 方案
Histogram	直方图
History Free	无记录
History Variable	历史变量
HMAC	Hash Message Authentication Code 基于哈希的信息认证码
Holocryptic	难解的
Holomorph	全形
Homogeneous	齐次的
Homomorphic	同态的
Homomorphic Commitment	同态承诺
Homomorphic Cryptosystem	同态加密系统
Homomorphic Encryption	同态加密
Homomorphic Encryption System	同态加密系统
Homomorphic Evaluation	同态计算
Homomorphic Secret Sharing	同态秘密共享
Homomorphic Signature	同态签名

Homomorphic Trapdoor Commitment	同态陷门承诺
Homomorphically	同态地
Homomorphism	同态，同质
Homomorphism Extraction Property	同态提取性质
Homophone	同音异性异义字
Honest but Curious Adversary	诚实但好奇的对手
Honest Party	诚实方
Honest-but-Curious Setting	诚实但好奇设置
Honeypot	蜜罐技术
Host	主机
Host Security	主机安全
Hot Site	热站
Hot Wash	热水洗（事件或危机过后的情况说明）
HSM	High Speed Memory 高速存诸器
HTTP	Hyper Text Transfer Protocol 超文本传输协议
Hua's Identity	华氏算子
Hua's Theorem	华氏定理
Hull	凸包
Human Threat	人类威胁
Hurwitz's Problem	赫尔维茨的问题
Hybrid Primitive	混合式原语
Hybrid Security Control	混合安全控制
Hyperbolic Plane	双曲面
Hyper Determinant	超行列式
Hyperelliptic Cryptosystem	超椭圆密码系统
Hypergeometric Distribution	超几何分布
Hypertext Transfer Protocol	超文本传输协议
Hypotenuse	斜边

I

IA Architecture	信息安全建构
IA Infrastructure	信息安全基础设施
IA Product	信息安全产品
IA-Enabled Information Technology Product	信息安全可行的信息科技产品
IA-Enabled Product	信息安全可行性产品
IBIP	Information-Based Indicia Program 基于情报的标记项目
IBS	Intelligent Building System 智能建筑系统
ICC	International Computation Centre 国际计算中心，International Copyright Convention 国际版权公约
ICMP	Internet Control Message Protocol 互联网控制消息协议
ID	身份证件
IDEA	International Data Encryption Algorithm 国际数据加密算法
Ideal Box	理想盒
Ideal Cipher	理想密码
Ideal Lattice	理想格
Ideally Secure Hash Function	理想的安全散列函数
Idempotent Element	幂等元
Identifiable Parent Property Code	可认定父元码
Identification	识别

Identification Scheme	身份认证方案
Identifier	识别符
Identity	身份，同一性，恒等式
Identity Based Cryptosystem	基于身份的密码系统
Identity Based Encryption	基于身份的加密
Identity Based Scheme	基于身份的方案
Identity Based Signature	基于身份的签名
Identity Binding	身份绑定
Identity Escrow Scheme	身份托管方案
Identity Management	身份管理
Identity Proofing	身份检验
Identity Provider	身份供应商
Identity Registration	身份注册
Identity Theft	身份盗用
Identity Token	身份令牌
Identity Uniqueness	身份唯一性
Identity Validation	身份校验
Identity Verification	身份验证
Identity Verification Protocol	身份认证协议
Identity-Based	基于身份的
Identity-Based Access Control	基于身份认证的访问控制
Identity-Based Encryption	基于身份的加密
Identity-Based Non-Interactive Key Exchange	基于身份的非交互密钥交换
Identity-Based Security Policy	基于身份验证的安全策略
IDS	Intrusion Detection Systems 入侵监测系统
IEEE	Instituteof Electrical And Electronic Engineers 电气与电子工程协会

IEMP	Integrated Enterprise Management Program 整合的企业管理项目
IETF	Internet Engineering Task Force 互联网工程任务组
IKE	Internet Key Exchange 互联网密钥交换
Image	图像
Imaginary Number	虚数
Imbalance	不平衡，失调
Imitative Communications Deception	模仿通信欺骗
IMP	Incident Management Plan 事件管理计划
Impact	冲击
Impact Level	冲击等级
Impact Value	冲击值
Imperfect Randomness	不完美随机性
Impersonation Attack	模拟攻击
Implant	植入
Impossible Cryptanalysis	不可能的密码分析
Impossible Differential Attack	不可能差分攻击
Improved Davies Attack	改良的戴维斯进攻
Inactive	不活跃的
In a Principal Ideal Domain	在一个主要理想域中
In an Extended Setting	在扩展的条件下
In the Symmetric Group	在对称群中
Inadvertent Disclosure	疏忽泄密
Incident Handling	事故处理
Incident Management Plan	事件管理计划
Incident Response Plan	应急响应方案
Inclusion-Exclusion Method	容斥方法

Incomplete Parameter Checking	不完整参数校验
Incremental Deterministic	高确定性
Incremental Hash Function	增强的哈希函数
Inculpatory Evidence	定罪证据
Incur	引发，遭受
IND-CCA Secure Cryptography	IND-CCA 安全的密码体制
IND-CCA2 Security	IND-CCA2 安全性
IND-CPA Secure Public-Key Cryptography	IND-CCA 安全的公钥密码体制
Indecomposable	不可分解的
Independent Key	独立密钥
Independent Round-Key	独立的轮密钥
Independent Subkey	独立子密钥
Independent Validation Authority（IVA）	独立验证机构
Independent Verification & Validation（IV&V）	独立验证与确认
Indeterminate	不定元
Index	指标
Index Calculus Algorithm	指标计算算法
Index Calculus Variant	指标计算变量
Index of Coincidence	重合指数
Index-Calculus Method	指标计算方法
Indicator	指标
Indifferentiability	不可辨别特性
Indifferentiability Framework	不可辨别性框架
Indifferentiability Style	不可辨别性风格

Indirect Leakage	间接泄露
Indirect Payment System	间接支付系统
Indistinguishability of Encryption	加密的不可分辨性
Indistinguishable	不可区别的
Individual	个体
Individual Accountability	个体责任
Individual Conversion Operation	个体换算操作
Individual Key	个体密钥
Induce	引起，诱导
Induction Proof	归纳证明
Industrial Control System	工业控制系统
Inert Prime	惯性素数
Inferential Power Analysis	推论性的功率分析
Infinite Domain	无限域
Infinitely Many Primes Theorem	无穷多素数定理
Informal Security Policy	非正式安全策略
Information	信息
Information Asset	信息资产
Information Assurance（IA）	信息安全保障
Information Assurance（IA）Professional	信息安全保障专业人员
Information Assurance Component（IAC）	信息安全保障组件
Information Assurance Manager（IAM）	信息安全保障经理
Information Assurance Officer（IAO）	信息安全保障官

Information Assurance Vulnerability Alert (IAVA)	信息安全保障脆弱性预警
Information Based Indicia Program	基于信息的标记项目
Information Domain	信息域
Information Environment	信息环境
Information Flow Control	信息流控制
Information Hiding	信息隐蔽
Information Integrity	信息完整
Information Leakage	信息泄露
Information Leaking	信息泄露
Information Management	信息管理
Information Operations (IO)	信息操作
Information Owner	信息所有者
Information Reconciliation	信息协调
Information Resource	信息资源
Information Resources Management (IRM)	信息资源管理
Information Retrieval	信息检索
Information Security	信息安全
Information Security Architect	信息安全架构师
Information Security Architecture	信息安全结构，信息安全体系结构
Information Security Continuous Monitoring (ISCM)	信息安全持续监视
Information Security Continuous Monitoring (ISCM) Process	信息安全持续监视程序
Information Security Policy	信息安全策略
Information Security Program Plan	信息安全项目方案

Information Security Risk	信息安全风险
Information Set Decoding	信息集译码
Information Sharing	信息共享
Information Sharing Environment	信息共享环境
Information Steward	信息管理员
Information Symbol	信息符号
Information System	信息系统
Information System Boundary	信息系统边界
Information System Contingency Plan（ISCP）	信息系统应急计划
Information System Life Cycle	信息系统寿命周期
Information System Owner（or Program Manager）	信息系统物主（或程序管理员）
Information System Resilience	信息系统弹性
Information System Security Officer（ISSO）	信息系统安全官
Information System-Related Security Risk	信息系统相关的安全风险
Information Systems Security（INFOSEC）	信息系统安全
Information Systems Security Engineer（ISSE）	信息系统安全工程师
Information Systems Security Engineering（ISSE）	信息系统安全工程学
Information Systems Security Equipment Modification	信息系统安全设备调试
Information Systems Security Manager（ISSM）	信息系统安全经理

Information Systems Security Officer（ISSO）	信息系统安全官
Information Systems Security Product	信息系统安全产品
Information Technology	信息技术
Information Technology Security Evaluation Criteria	信息技术安全评估标准
Information Theoretic Security	信息理论上的安全
Information Theoretically Secure Computation	信息理论安全计算
Information Theory	情报理论
Information Type	信息品种，信息类型
Information Value	信息价值
Information-Set Decoding	信息集译码
Information-Theoretic Setting	信息论背景
Infrastructure	基础设施
Ingemarsson-Tang-Wong Protocol	Ingemarsson-Tang-Wong 协议
Ingress Filtering	入口过滤
Inherent	固有的
Inheritance	遗产，继承
Inhibit Any Policy Extension	禁止任何策略扩展
Inhibit Any Policy Indicator	约束任意政策指标，禁止任何政策指标
Initial Noise Level	初始噪声水平
Initial Policy Set	最初的策略集
Initial Randomness	初始随机性
Initial State	初始状态
Initialization Vector（IV）	初始化向量，初始矢量

Initialize	初始化
Initiator	启动程序，发起人
Injective	单射的
Injective Tag	单射标签
In-Line TTP	内嵌式进展时间（TTP = Time to Progression）
Inner	内部的
Inner Automorphism	内自同构群
Inner CBC	内部 CBC
Inner Mode	内在模式
Inner Product	内积
Inner Product Encryption	内积加密
Inner Product Masking	内积掩蔽
Input	密钥输入
Input Indistinguishable Computation	输入不可区分（IIC）的计算
Input Length	输入长度
Input Value	输入值
Input-Size Hiding Security	输入长度隐藏安全
Inside-Out Attack	由内向外攻击
Inputless Functionality	无输入泛函数性
Inside Threat	内在威胁，内部威胁
Insider Secure	内部安全
Inspectable Space	可检查的空间
Instantiate	例示，举例说明
Instantiation	实例化，例示
Integer	整数
Integer Factoring	整数分解

Integer Factorization	整数分解
Integer Polymatroid	整数多矩阵类
Integer Polynomial	整数多项式
Integer（z）	整数集 z
Integral Attack	积分攻击
Integral Distinguisher	积分区分器
Integrity	完整，完整性
Integrity Check Value	完整性校验值
Integrity-Aware Cipher Block Chaining	完整性意识的密码分组链接
Integrity-Aware Parallelizable Mode	完整性意识的并行模式
Intellectual Property	知识产权
Interactive	可交互的
Interactive Argument	交互式论证
Interactive Proof	交互式校验
Interactive Protocol	交互协议
Interactive VSS	交互式车速传感器（VSS = Vehicle Speed Sensor）
Interact	互动
Interconnection Security Agreement（ISA）	互联安全协议
Interface	界面
Interface Control Document	界面控制文件
Interim Approval to Operate（IATO）	临时操作许可
Interim Approval to Test（IATT）	临时测试许可
Interleaved Mode	交错模式

Interleaved Sliding Window Exponentiation	交叉式的滑动窗乘方
Intermediate Certification Authority	中间认证机构
Intermediate Value	中间值
Internal Collision Attack	内部碰撞攻击
Internal Network	内部网络
Internal Secret Key	内部秘钥
Internal Security Control	内部安全控制
Internal Security Testing	内部安全测试
Internal-State	中间状态
International Telecommunication Union	国际电信联盟
Internet	因特网
Internet Engineering Task Force	因特网工程任务组
Internet Key Exchange	互联网密钥交换
Internet Protocol（IP）	互联网协议
Internet Relay Chat（IRC）	因特网中继聊天
Internet Security Association-and Key	因特网安全关联和密钥
Interoperability	互通性，互用性
Interpolation Attack	篡改进攻，插值攻击
Intersection	交集
Intervals in a Lattice	一个格的间隔
Intranet	内联网
Intra-Slice Dispersion Step	内部片分散步骤
Intrinsic Non-Programmability	内在不可编程性
Intrinsic Value	内在值，固有价值
Intrusion	侵入，入侵

Intrusion Detection	入侵侦测
Intrusion Detection and Prevention System（IDPS）	入侵检测和预防体系
Intrusion Detection Systems（IDS）（Host-Based）	（基于主机的）入侵检测系统
Intrusion Detection Systems（IDS）（Network-Based）	（基于网络的）入侵检测系统
Intrusion Prevention System（s）（IPS）	入侵防御体系
Invariance Under Decimation	大量毁坏下的不变性，抽样的不变性
Invariant Factor	不变的因素
Invariant Subspace Attack	不变子空间攻击
Invasive Attack	侵入进攻
Inverse	倒转，求逆
Inverse Cipher	倒转密码
Inverse Fourier Relation	逆傅立叶关系
Inverse Image	逆图像
Inverse of Matrix	逆矩阵
Inversion	逆运算
Inversion Attack	逆序对进攻
Inversionin Finite Field	有限域的逆序对
Invertibility	可逆性
Invertible Element（or Unit）	可逆元（或单元）
Invertible Function	可逆函数
Invisibility	隐形，不可见的
Invocation	调用
Involution	内卷，乘方，对合
IP	Internet Protocol 互联网协议
IP Security（IPSEC）	互联网协议安全性

IPA	Intermediate Power Amplifier 中间功率放大器
IPES	Improved Proposed Encryption Standard 改进型推荐加密标准
IPSEC	Internet Protocol Security 网际安全协议
IQ	Indistinguishable Qbfuscation 可不区分混淆
IRC	Internet Relay Chat 网络中继聊天
Irrational Number	无理数
Irrationality	无理性
Irreducible	不可约
Irreducible Element	不可约元素
Irreducible Polynomial	不可约多项式
ISAKMP	Internet Security Association and Key Management Protocol 安全连接和密钥管理协议
ISO	International Standardization Organization 国际标准化组织
ISO Standard Hash Function	ISO 标准散列函数
Isogeny	同源
Isolog	同构异素体
Isometry	等距，等容
Isomorph	同构
Isomorphism	同构，类质同像，同形性
Isomorphism of Polynomial	多项式同构
Isomorphism Theorem	同构定理
Isotropic	等方性的，各向同性的
Issuer	发行人
IT Auditor	信息技术审计师
IT Security Architecture	信息技术安全结构
IT Security Awareness	信息技术安全意识

IT Security Awareness and Training Program	信息技术安全意识及训练项目
IT Security Education	信息技术安全教育
IT Security Investment	信息技术安全投资
IT Security Metrics	信息技术安全权值
IT Security Policy	信息技术安全策略
IT Security Training	信息技术安全训练
ITA	International Telegraph Alphabet 国际电报电码表
Iterate	迭代
Iterated Attack	迭代攻击
Iterated Cipher	迭代密码
Iterated Even-Mansour Cipher	迭代 Even-Mansour 密码
Iterated Hash Function	迭代哈希函数
Iterated Merkle-Hellman Scheme	迭代式 Merkle-Hellman 机制
Iterative Cipher	迭代密码
ITIL	Information Technology Infrastructure Library 信息技术基础构架库
Itoh-Tsujii Inversion Algorithm	伊藤辻井反演算法
IT-Related Risk	信息技术相关风险
ITSEC	信息技术安全评估准则
ITU	International Telecommunication Union 国际电信联盟
IV（Initial Value）	初始值
Ivy Bridge（IVB）	架构处理器

J

Jacobi Sum Test	雅可比和验证
Jacobi Symbol	雅可比符号
Jacobi's Identity	雅可比恒等式
Jacobson-Rickart Theorem	雅各布—森里卡特定理
Jamming	干扰，抑制，卡住
Java	Java 程序设计语言
JavaScript	Java 脚本语言
JCP	Java Community Process Java 社区过程（负责 Java 发展的开放组织）
Jenning Generator	Jenning 发生器
Joint Authorization	联合授权
Joint Function	联合函数
Joint Security	联合安全性
Jointly Compute Some Functionality	协同计算出某个功能性
Jordan	约当（人名）
Jordan Canonical Form（or Matrix）	约当标准型，约当范式（或矩阵）
Jordan Homomorphism	约当同态
Jordan Identity	约当恒等式
Jordan Product	约当积
Jordan-Holder Theorem	Jordan-Holder 定理
Jordan-Holder-Dedekind Theorem	Jordan-Holder-Dedekind 定理

K

Kahn's Maxim	卡恩原理
Kappa Test	Kappa 检验
Karatsuba Algorithm（KA）	Karatsuba 算法
Kasiski's Method	Kasiski 方法
Kasumi	Kasumi 密码
K-Bit Key	K 位键
KCDSA	Korean Certificate-Based Digital Signature Algorithm 韩国基于证书数字签名算法
KDC	Key Distribution Center 密钥分配中心，密钥分发中心
KEM	Key Encapsulation Mechanism 密钥封装机制
Kerberos	麻省理工学院开发的安全认证系统，第三方加密验证
Kerberos Authentication Protocol	Kerberos 认证协议
Kerckhoff's Maxim	Kerckhoff 原理
Kernel（of Homomorphism）	内核（同态的）
Kernel	内核
Key	密钥
Key Agreement	密钥协商，密钥协定
Key Alphabet	密钥字母表
Key Alternating Cipher	密钥交替密码
Key Authentication	密钥认证
Key Bits	密钥比特

Key Bundle	密钥束
Key Confirmation	密钥确认
Key Dependent Message	依赖密钥消息
Key Dependent Message Resilience	密钥相关的消息弹性
Key Dependent S-Box	密钥相关 S 盒
Key Derivation	密钥分发
Key Derivation Function	密钥推导函数
Key Difference Invariant Bias	密钥差分常量偏移
Key Directive	密钥指令
Key Distinguisher	密钥区分器
Key Distribution Center （KDC）	密钥分配中心，密钥分发中心
Key Encapsulation	密钥封装
Key Encapsulation Mechanism （KEM）	密钥封装机制
Key Encryption Key （KEK）	密钥加密密钥
Key Escrow	密钥托管，密钥托管法
Key Escrow System	密钥托管系统
Key Establishment	密钥建立，密钥创建
Key Establishment Protocol	密码创建协议
Key Evolution Scheme	密钥演变方案
Key Evolving System	密钥进化系统
Key Exchange	密钥交换
Key Exchange Protocol	密钥交换协议
Key Expansion	密钥扩展
Key Generation	密钥产生
Key Generation Algorithm	密钥生成算法
Key Generation Material	密钥生成材料

Key Graph	密钥图
Key Group	密钥组
Key Homomorphic	密钥同态
Key Indistinguishability-Based Security Model	基于密钥不可区分性的安全性模型
Key List	密钥列表
Key Loader	密钥装入器，密钥载入器
Key Logger	键盘记录器，击键记录器
Key Management	密钥管理
Key Management Device	密钥管理设备
Key Management Infrastructure （KMI）	密钥管理基础设施
Key Mixing	密钥混合
Key Negotiation	密钥协商
Key Pair	密钥对
Key Phrase	密钥短语
Key Production Key （KPK）	密钥生成器，启动密钥
Key Rank Estimation Algorithm	密钥列评估算法
Key Ranking	密钥排序
Key Recovery	密钥恢复
Key Recovery Attack	密钥恢复攻击
Key Refresh	密钥更新
Key Revocation	密钥撤销
Key Schedule Algorithm	密钥生成方案算法
Key Schedule Attack	密钥方案攻击
Key Scheduling Function	密钥编排函数
Key Size	密码长度
Key Space	密钥空间
Key Stream	密钥流

Key Switching Technique	密钥转换技术
Key Tag	密钥标记
Key Tape	密钥带
Key Text	密码文本，密码文件
Key Token	密钥令牌
Key Translation	密钥转换
Key Transport	密钥传输，密钥传送
Key Update	密钥更新
Key Update Broadcast	密钥更新广播
Key Whitening	密钥白化（一种增加密钥长度的方法）
Key Whitening Step	密钥白化步骤
Key Wrap	密钥包
Keyed-Hash Based Message Authentication Code (HMAC)	基于带密钥哈希函数的消息认证代码
Keying Material	密钥材料
Key-Length Extension	密钥长度扩展
Keynote	一种演示幻灯片的应用软件
Keystroke Logger	击键记录器
Keystroke Monitoring	击键监控，按键监控
K-Fold Transitivity	K 重传递
K-Homogeneous Access Structure	K 齐次方程访问结构
Kleptography	窃取术
KMI Operating Account (KOA)	密钥管理基础设施操作账户，KMI 操作账户
KMI Protected Channel (KPC)	KMI 保护信道，密钥管理基础设施保护信道
KMI-Aware Device	KMI 感知设备

KN Cipher	Knudsen-Nyberg 密码
Knapsack Cryptographic Scheme	背包密码方案
Knapsack	背包
Knapsack Problem	背包问题
Knowledge Extractor	知识提取器
Knowledge Protocol	知识协议
Known Plaintext Attack	已知明文攻击
Known Related Key	已知相关密钥
Knudsen-Preneel Compression Function	Knudsen-Preneel 压缩函数
Knuth-Schroeppel Function	Knuth-Schroeppel 函数
KOA Agent	KOA 用户
KOA Manager	KOA 经理
KOA Registration Manager	KOA 注册经理
Koblitz Curve	Koblitz 曲线
Korselt's Criterion	靠赛特判别法
Kummer Surface	库默尔曲面

L

L2TP	Layer Two Tunneling Protocol 第二层隧道协议
Label	标签
Labeled Security Protection	有标记安全保护
Laboratory Attack	实验攻击
Lagarias and Odlyzko Attack	Lagarias-Odlyzko 攻击
Lagrange Interpolation Formula	拉格朗日插值公式
Lagrange Resolvent	拉格朗日的解决方案
Lagrange's Theorem	拉格朗日定理
Lambda Representation	兰布达表示法，匿名表示法
LAN	Local Area Network 局域网
Langlands Program	朗兰兹纲领
Language	（编程）语言
LAN Recovery	局域网复苏
Laplace Expansion of a Determinant	行列式的拉普拉斯展开
Large Dataset	大型数据集
Latin Alphabet	拉丁字母表
Latin Square	拉丁方阵
Lattice	格
Lattice Based Cryptography	基于格的密码学
Lattice Cryptographic Primitive	格密码基本组件
Lattice Cryptography	格密码学

Lattice Interpretation	格基假设
Lattice Problem	格问题
Lattice Reduction	格基规约
Lattice Sieve	格筛
Lattice Sieving	格筛查
Lattice Signature	格签名
Lattice Signature Scheme	格签名方案
Lattice World	格域
Lattice-Based	基于格的
Lattice-Based Cryptography	基于格的密码学
Law of Quadratic Reciprocity	二次互反律
Law of The Excluded Middle	排中律
Layered Subset Difference	分层子集差异
Laziness Technique	惰性技术
Lazy Reduction	懒惰化简
Lazy Verification	懒惰验证
LCM	Lowest Common Multiple 最小公倍数
LDAP	Lightweight Directory Access Protocol 轻型目录访问协议
Leakage	泄漏
Leakage Function	泄漏函数
Leakage Model	泄漏模型
Leakage Resilience	泄漏弹性
Leakage Resilient Cryptography	弹性泄漏密码学
Leakage Resilient Masking Scheme	泄漏弹性的掩蔽策略
Leakage Resilient Cryptosystem	泄漏弹性密码系统

Leakage Resilient Zero Knowledge	泄漏弹性零知识
Leaked State Forgery Attack (LSFA)	泄漏状态伪造攻击
Leak-Free Component	无泄漏组件
Leaky Token Model	泄漏令牌模式
LEAP	Lightweight Extensible Access Protocol 轻量级可扩展访问协议
Learning Parity with Noise (LPN)	伴噪奇偶性学习
Learning Parity with Noise Problem	伴噪奇偶性学习问题
Learning with Errors (LWE)	伴错学习
Leased Line	专用线路
Least Common Multiple (LCM)	最小公倍数
Least Privilege	最小特权
Least Trust	最小信任
Left Multiplication	左乘
Left Translation	左平移
Leftover Hash Lemma (LHL)	剩余散列引理
Left-to-Right Exponentiation	向左或向右取幂
Legal Structure	合法架构
Legendre Polynomial	勒让德多项式
Legendre Symbol	勒让德符号
Lehmer's Euclidean Algorithm	莱默的欧几里得算法
Lemma	辅助定理，辅助命题，引理
Length	长度

Length-Bounded Leakage	长度有界的泄漏
Lenstra Lovâsz Lattice Reduction	Lenstra Lovâsz 格规约
Level of Concern	关注等级
Level of Protection	保护等级
Level of Security	安全级别
Lexicographic Order	词典顺序
Lexicographical Knapsack	字典序背包
LFSR	Linear Feedback Shift Register 线性反馈移位寄存器
L'hopital's Rule	洛必达法则
License	执照，证书
Licensee	持照人
Lie Product （or Additive Commutator）	Lie 积（或加性交换子）
Lightweight	轻量级
Lightweight Block Cipher	轻量级分组密码
Lightweight Encryption Solution	轻量级加密方案
Lightweight Hash Function Family	轻量级哈希函数族
Likelihood	可能性，似然
Likelihood of Occurrence	事件发生的可能性
Limited Maintenance	受限维护
Limited Quantum Side Information	有限量子边信息
Limited Remote Access	有限的远程访问
Lindemann-Weierstrass Theorem	Lindemann-Weierstrass 定理

Line Conditioning	线路调节
Line Conduction	线路传导
Line of Business	行业，营业范围
Linear	线性的
Linear Approximation	线性近似
Linear Barrier	线性屏障
Linear Bias	线性偏差
Linear Characteristic	线性特征
Linear Code	线性码
Linear Complexity	线性复杂性
Linear Complexity Profile	线性复杂性分布图
Linear Congruence Theorem	线性同余定理
Linear Congruential Generator	线性同余发生器
Linear Consistency Attack	线性一致性攻击
Linear Cryptanalysis	线性密码分析
Linear Cryptanalysisfor Block Ciphers	分组密码线性分析
Linear Cryptanalysisfor Stream Ciphers	序列密码线性分析
Linear Equation	线性方程
Linear Equation Theorem	线性方程定理
Linear Error-Correcting Code	线性纠错码
Linear Feedback Shift Register	线性反馈移位寄存器
Linear Function	线性函数
Linear Gap	线性间隙
Linear Group	线性群
Linear Hull	线性壳

Linear Message Expansion	线性消息扩展
Linear Mixing Layer	线性混合层
Linear PCP	线性 PCP
Linear Probability	线性概率
Linear Recurrence Sequence	线性递归序列
Linear Secret Sharing	线性秘密共享
Linear Sieve	线性筛
Linear SSS	线性秘密共享方案
Linear Structure	线性结构
Linear Substitution	线性替换
Linear Syndrome Attack	线性伴随式攻击
Linear Time	线性时间
Linear Time Algorithm	线性时间算法
Linear Transformation	线性变换
Linearly Homomorphic Signature	线性同态签名
Line Rerouting	线路重编路由
Line Voltage Regulator	线路电压调节器
Link Encryption	链路加密
Linking	链接
Liouville Number	刘维尔数
Liouville's λ Function	刘维尔λ函数
Liouville's λ Inequality	刘维尔λ不等式
List Decoding	列表译码
List Oriented	清单导向的
List-Decoding Technique	列表译码技术
LKH	Logical Key Hierarchy 逻辑密钥层次
LLL Lattice Reduction Algorithm	LLL（Lenstra，Lenstra，and Lovasz）格规约算法

L Notation	L 符号
Local	局域，定域
Local Access	本地接入
Local Area Network （LAN）	局域网
Local Authority	本地授权
Local Collision	局部碰撞
Local Deduction	本地规约
Local DOS Attack	本地拒绝服务攻击
Local Management Device/ Key Processor （LMD/KP）	本地管理装置/密钥处理器
Local Policy	本地政策
Local Registration Authority （LRA）	本地等级授权
Lock-Dependent Message	锁依赖消息
Logarithmic	对数
Logarithmically	对数地
Logic Bomb	逻辑炸弹
Logical Attack	逻辑攻击
Logical Completeness Measure	逻辑完整性测量
Logical Key Hierarchy Scheme	逻辑密钥层次方案
Logical Perimeter	逻辑周界
Login	登录，进入系统
Login ID	登录用户名
Logon	登录，注册
Logon Banner	登录标语
Long Title	长名称
Longevity	寿命

Long-Integer Arithmetic	长整型计算
Long-lived Broadcast Encryption	长命广播加密
Long-Term Key	长期密钥
Loose Reduction	松散规约
Loss	损耗
Loss Factor	损失因子
Loss Reduction	降低损耗
Lossy Code	有损编码
Lossy Encryption	有损加密
Lossy Function	损失函数
Lossy Identification Schemes	有损身份认证方案
Lossy Trapdoor Function (LTF)	有损陷门函数
Low Communication	低交互，较少通信量
Low Data Complexity	低数据复杂度
Low Density Knapsack	低密度背包
Low Depth	低深度
Low Depth Arithmetic	低深度算术
Low Differential Probability	低差分概率
Low Entropy	低熵
Low Exponent	低指数
Low Impact	低影响力
Low Impact System	低影响力系统
Low Latency Block Cipher	低延迟分组密码
Low Latency Cipher	低等待时间密码
Low Probability of Detection	低发现概率，低检测概率
Low Probability of Intercept	低拦截概率
Low Sensitivity	低灵敏度

Lower and Upper Bound	上下界
Lower Bound	下界
Lower Bound Proof	下界论证
LRA	Logical Record Access 逻辑记录存取法
LSD	Least Significant Digit 最小意义数字
LSSS	Limiting Safety System Setting 有限安全系统设置
Lubyrackoff Cipher	Lubyrackoff 密码
Lucas Probable Prime Test	Lucas 可能质数测试
Lucas Sequence	卢卡斯序列
Lucas Lehmer Primality Test	Lucas Lehmer 素性测试

M

MAA	Message Authentication Algorithm 报文认证算法
MAC	Message Authentication Code 消息认证代码
MAC Algorithm	MAC 算法
MAC Guessing Attack	MAC 猜测攻击
Macro Virus	宏病毒，巨集病毒
MAC-then-Encrypt	MAC 后加密
MAC-Verification Attack	MAC 验证攻击
Magnetic Remanence	顽磁，剩磁
Main Mode IPSEC	主模式网际协议安全（Internet Protocol Security）
Maintenance Hook	维护陷阱
Maintenance Key	维护密钥
Major Application	关键应用程序
Major Information System	关键信息系统
Malcev's Example	马尔策夫的例子
Malicious Adversary	恶意对手，恶意攻击者
Malicious Applets	恶意（小）程序
Malicious Code	恶意代码（程序、固件、病毒等）
Malicious Logic	恶意逻辑（程序、固件等）
Malicious Party	恶意方
Malleable	可塑的，有延展性的
Malleable Encryption Scheme	可塑加密方案
Malleable Proof System	延展性证明系统
Malware	恶意软件，恶意程序

MAN	Metro Area Network 城域网
Management Client（MGC）	管理客户（平台、架构）
Management Control	管理控制
Management Protocol	管理协议
Management Security Control	管理安全控制
Mandatory Access Control （MAC）	强制访问控制，强制存取控制
Mandatory Modification	强制修改
Man-In-The-Middle （MIM） Attack	中间人攻击
Manipulated Data	操作数据
Manipulation	操控，操作，处理
Manipulation Detection Code （MDC）	修改检测码（多指无密钥的 Hash）
Manipulative Communications Deception	操作通信鉴别
Manual Cryptosystem	手工密码系统
Manual Key Transport	手工秘钥传送
Manual Remote Rekeying	手工远程秘钥更新
Map（or Mapping）	图，映射
Map Coloring Problem	地图着色问题
Mark Copyrighted Content	标注有版权保护内容
Marking	标示，标注，标识
Marking Assumption	标记假设
Markov Chain	马尔科夫链
MARS	由 IBM 设计的一种分组密码
MASH Function	MASH 函数
Mask Generating Function	掩码生成函数
Masked Implementation	掩码

Masquerading	冒充，伪装
Master Copy Control	主拷贝控制
Master Cryptographic Ignition Key	主密码启动密钥
Master Key	管理锁，万能钥匙系统，对系统有最高权利的钥匙
Master Secret Key	主秘钥
Match	匹配，比对
Matching Algorithm	匹配算法
Matching Ciphertext Attack	相匹配的密文攻击，对应密文攻击
Matching Module	匹配模块，对应模块
Mathematical Induction	数学归纳法
Mathieu Group	马蒂厄群
Matrices	矩阵（复数）
Matrix	矩阵
Matrix Addition	矩阵加法
Matrix Representation	矩阵表示
Matrix Ring	矩阵环
Matrix Unit	矩阵单元，矩阵单位
Mattson-Solomon Polynomial	马森所罗门多项式
Maurer's Method	毛雷尔方法
Maurer's Universal Statistical Test	毛雷尔的通用统计测试法
Maxim	格言，箴言
Maxim Number One	密码安全第一格言（永远不能低估对手）
Maximal	最高的，持续时间最长的
Maximally Entangled State	最大纠缠态
Maximum Correlation	最大相关法
Maximum Distance Separable Code	最大距离可分码

Maximum Number of Rounds	最大轮数
Maximum Order Complexity	最大阶复杂度
Maximum Tolerable Downtime	最大可容忍停机时间
Maximum-Length Linear Sequence	最大长度的线性序列
May Attack	May（人名）攻击
McEliece Public Key Cryptosystem	McEliece 公钥密码系统
Mcgrew-Sherman OFT Protocol	Mcgrew-Sherman OFT 协议
MD2 Hash Function	MD2 哈希函数
MD4-MD5	MD4-MD5 哈希函数
MD5 Hash Function	MD5 哈希函数
MDC Hash Function	MDC 哈希函数
MDC-2 and MDC-4	MDC-2 和 MDC-4 哈希函数
MDS Code	MDS 码（最大距离可分码）
MD-SHA Family	MD-SHA（哈希函数）族
MDX-Family	MDX 族（包含最流行的哈希函数）
Mechanism	机制
Media	传输介质
Media Access Control	介质访问控制，媒体存取控制，媒体访问控制
Media Sanitization	介质处理（使数据不可恢复）
Median	中位数
Meet-in-the-Middle	中间相遇
Meet-in-the-Middle Attack	中间相遇攻击
Meet-in-the-Middle Technique	中间相遇技术
Member Pseudonym	会员假名

Membership Test	隶属测试
Memorandum of Understanding/Agreement（MOU/A）	（确保系统安全互通的）谅解备忘录
Memory	存储信息
Memory Delegation	存储授权，存储委托
Memory Leakage	内存泄漏
Memory Scavenging	记忆清除，收集数据残留
Memory Size	内存大小，存储容量
Memoryless Attack	无内存攻击
Merchant CA	商户认证中心
Merkle Tree	Merkle 树，Merkle 哈希树
Merkle's Meta-Method	Merkle 的元方法
Merkle-Damgard Strengthening	Merkle-Damgard 强化
Merkle-Hellman Dominance	Merkle-Hellman 支配
Merkle -Hellman Transformation	Merkle-Hellman 变换
Merkle-Hellman Trapdoor	Merkle-Hellman 陷门
Mersenne Number	梅森数
Mersenne Prime	梅森素数，梅森质数
Message Authentication	消息认证
Message Authentication Code（MAC）	消息认证码，信息认证码
Message Authentication Algorithm	信息认证算法
Message Block	消息块
Message Digest	信息摘要，消息摘要
Message External	正文外部信息（如页眉、注脚等）
Message Indicator	信息指示码

Message Length Attack	消息长度攻击
Message Modification Technique	消息修改技术
Message Recovery	消息恢复
Message-Encrypting Key	消息加密密钥
Message-Locked Encryption (MLE)	消息锁定加密
Meta-Reduction	元规约
Metric	度量
Meyer-Schilling Hash Function	Meyer-Schilling 哈希函数
Micro-Controller	微型控制器
Microelectronic	微电子的
Microprobing	微探测
Miller-Rabin Probabilistic	Miller-Rabin 概率的
Million Message Attack	百万消息攻击
MIME	Multimedia Internet Mail Extensions 多媒体网际网路邮件延伸
Mimicking	仿制，电子欺骗
Min-Entropy	最小熵
Minimal Assumption	最小假设
Minimal Condition	最小条件
Minimal Polynomial	最小多项式
Minimalism	极简主义
Minimalist Cryptography	极简主义密码学，极简主义密码
Minimum Distance	最小距离
Minimum Polynomial	最小多项式
Minkowski Lattice Reduction	闵可夫斯基格基规约
Minkowski's First Theorem	闵可夫斯基第一定理

Min-Max Theorem	最小最大定理
Minor Application	次要应用程序
MIPS-Year	MIPS 年（密码计算量的测量单位，MIPS = Million Instructions Per Second 每秒百万条指令）
Misnamed File	错误名文件
Miss-in-the-Middle Attack	中间错过攻击
Mission Assurance Category (MAC)	分类取代任务保证类别
Mission Critical	关键任务
MISTY1	MISTY1 分组密码
Misuse	误用，不当使用
Mitigate	减弱，减轻
Mitigating Control	减弱性控制
Mitigating Factor	减弱风险因素
Mix Network	混合网络
Mixed Alphabet	混乱排列字母表
Mixing Time	混合时间
Mix-Net	混合网
Mix-Server	混合服务器
Miyaguchi-Preneel Hash Function	Miyaguchi-Preneel 哈希函数
Mobile Code	移动代码
Mobile Code Technology	移动代码技术
Mobile Device	移动（便携）设备，移动（便携）装置
Mobile Hot-Site	移动式热站
Mobile Software Agent	移动软件代理商
Mobius Function	莫比乌斯函数
Mobius Inversion Formula	麦比乌斯反演公式

Mode	模式，方法
Mode of Operation	运行方式，工作模式
Mode of Operation of a Block Cipher	分组密码的工作模式
Model of Computation	计算模型
Moderate Impact	中度影响
Moderate-Impact System	中度影响系统
Modification	修改，修正
Modular	模块化的，模的
Modular Addition	模加法
Modular Algorithm	模算法
Modular Arithmetic	模运算，模算术
Modular Arithmetic Circuit (MAC)	模算术电路
Modular Exponentiation	模幂运算
Modular Inverse	模逆
Modular Multiplication	模乘
Modular Order-Preserving Encryption	保持阶数的模加密
Modular Root	模方根
Modularity	模性
Modularity Conjecture	模猜想
Modularity Pattern	模型模式
Modularity Theorem	模定理
Module	模块，组件，模
Moduli	模数
Moduloan Inert Prime	模无效素数
Modulus	系数，模数
Modulus Switching	模数转换

Modulus-to-Error Ratio	模错误比率
Monad	单轴
MONDEX-Scheme	MONDEX 电子钱包方案
Monic Polynomial	首一多项式
Monitoring	监控，监听，检查
Monographic Substitution	单字符替换
Monoid	幺半群
Monomial	单项式
Monomorphism	单一同态
Monotone	单调
Monotone Minimal Perfect Hash Function	单调最小完美哈希函数
Monotone Signature	单调签名
MonPro Algorithm	MonPro 算法
Montgomery Arithmetic	蒙哥马利运算
Montgomery Exponentiation	蒙哥马利求幂
Montgomery Multiplication	蒙哥马利乘法
Montgomery Product	蒙哥马利乘积
Montgomery Reduction	蒙哥马利规约
Montgomery Representation	蒙哥马利表达
Montgomery Squaring	蒙哥马利平方
Moore's Law	摩尔定律
Mordell's Theorem	莫德尔定理
Morrison-Brillhart Method	Morrison-Brillhart 方法
Motivating Application	激励性的应用
Moufang's Identity	Moufang 的恒等式
MPQS	Multiple Polynomial Quadratic Sieve 因数分解法，多项式二次筛法
MQV Key Agreement Scheme	MQV 秘钥协商方案

M-Resilient	M 阶弹性
M-Sequence	M 序列
MTE	MAC then Encrypt 先 MAC 然后加密
Multi-Bit Constraint	多比特约束
Multicast	多播
Multicast Channel	多播信道
Multicast Encryption	多播加密，多向传输加密，组播加密
Multicast Graph	多播网络
Multicore Computation	多核计算
Multicore Execution	多核点乘
Multi-Dimensional Linear Attack	多维线性攻击
Multi-Dimensional Linear Distinguisher	多维线性区分器
Multi-Encryption	多重加密
Multi-Exponentiation	指数运算乘积
Multifactor Authentication	多因子认证，多重身份认证
Multigram Property	多表性质
Multi-Homogeneous Structure	多齐次结构
Multi-Hop Problem	多跳问题
Multi-Inbound Rebound Attack	多入射反弹攻击
Multi-Instance Security	多实例安全
Multilevel Device	多级设备，多重装置
Multilevel Mode	多级模式
Multilevel Security（MLS）	多级安全
Multilinear Map	多线性映射
Multipartite Substitution	多方置换，多方替换
Multiparty Computation	多方计算

Multi-Pass Challenge-Response Protocol	多道次呼叫应答协议
Multiple	倍数
Multiple Anagramming	多重字母易位
Multiple Bits DPA	多比特 DPA（Differential Power Analysis 差分功率分析）
Multiple Encryption	多重加密
Multiple Polynomial Quadratic Sieve	多个多项式二次筛法
Multiple Roots	重根
Multiple Security Levels (MSL)	多重安全等级
Multiple-Keys	多密钥
Multiplication	乘法
Multiplication Formula	乘法公式
Multiplication Function	积性函数
Multiplication Gate	乘法（与）门
Multiplication of Polynomial	多项式乘法
Multiplication Problem	乘性问题
Multiplication Property of Norm	范数的积性
Multiplication Table	乘法表
Multiplicative	乘法的
Multiplicative Group	乘法群
Multiplicative Inverse	乘法逆元素
Multiplicative Knapsack	乘法背包，乘积型背包
Multiplicative Monoid	乘法含幺半群
Multiplicative Secret Sharing	乘性密钥共享
Multiply	使……相乘

Multi-Precision Multiplication	多精密乘法
Multi-Precision Squaring	多精密平方
Multi-Prover Interactive Proof	多证明者交互证明
Multi-Query Collision Attack	多查询碰撞攻击
Multi-Releasable	可多次释放（信息）的
Multi-Round	多轮
Multi-Set Attack	多集攻击
Multi-Signature	多重签名
Multi-Step Shuffle	多步式置乱
Multi-Variable Polynomial	多元多项式
Multivariate Cryptanalysis	多变量密码分析
Multivariate Polynomial	多变量多项式
Multivariate Polynomial Ring	多元多项式环，多变量多项式环
Multivariate Public-Key Cryptography	多元公钥加密，多变量公钥密码
Multivariate Quadratic Polynomial	多元二次多项式，多变量二次多项式
Mutual Authentication	相互认证，双向认证
Mutual Identity Verification Protocol	相互的身份验证协议
Mutual Information	交互信息
Mutual Information Analysis	互信息分析
Mutual Suspicion	（保护共享数据上的）相互怀疑
Mutually Authenticate	相互认证
Mutually Suspicious	相互怀疑的
Mutually Unbiased Bases (MUBS)	相互无偏基

N

N Instances	N 个实例
N Parties	N 个参与方
NAF	Non-Adjacent Form（非相邻形式）
Name	名称，命名
Name Constraints Extension	名称约束扩展
Naming Authority	命名机构，命名授权
Nanometer	纳米，毫微米
Nanoscale	纳米级
Naor-Yung Double Encryption	Naor-Yung 双重加密
Naor-Yung Paradigm	Naor-Yung 范式
Narrow-Sense Envelope	狭义信封
Nash Equilibrium	纳什均衡
NAT	Network Address Translation 网络地址转换
National Bureau of Standards	（美国）国家标准局
National Information Assurance Partnership（NIAP）	（美国）全国信息安全保障合作方案
National Information Infrastructure	国家信息基础设施
National Security Emergency Preparedness Telecommunications Service	国家安全应急通信服务
National Security Information	国家安全信息
National Security System	国家安全系统
National Vulnerability Database（NVD）	（美国）国家安全隐患（漏洞）数据库

Natural Disaster	自然灾害
Natural Threat	自然威胁
Natural Integer	自然整数
Natural Logarithm	自然对数
Natural Number	自然数
Natural Number (n)	自然数集 n
N-Bit Block Size	N 比特的分组长度
NBS	National Bureau of Standards (美国) 国家标准局
Near Prime	近素数
Near-Collision	近似碰撞
Near-Linear	近似线性
Near-Optimal Mixed Strategy	近似最优混合策略
Near-Spherical Discrete Gaussian	近乎球型离散高斯分布
Nearest Vector Problem	最近向量问题
Nearly-Uniform Distribution	近似均匀分布
Needham-Schroeder Protocol	Needham-Schroeder 协议
Needs Assessment	需求评估
Need-to-Know	须知
Need-to-Know Principle	须知原则
Negative Integer	负整数
Negligible Detection Probability	可忽略检测概率
Neighbor-Disjoint Path	邻居不相交路径
Nema	瑞士军队在恩尼格码 (Enigma) 密码机基础上改进的一种密码机
NESSIE Project	NESSIE 计划
Net-Centric Architecture	网络中心建筑

Network	网络
Network Access	网络接入，网络访问
Network Access Control (NAC)	网络访问控制
Network Address Translation (NAT)	网络地址转换
Network Coding	网络编码
Network Connectivity	网络连接
Network Front-End	网络前端
Network Reference Monitor	网络基准监视器
Network Resilience	网络恢复能力
Network Security	网络安全
Network Security Officer	网络安全官
Network Sniffing	网络监听
Network Sponsor	网络安全保荐商
Network System	网络系统
Network Topology	网络连接拓扑结构
Network Weaving	网络迂回
New European Schemes for Signature, Integrity and Encryption (NESSIE)	新欧洲签名、完整性和加密研究计划
Newton's Identities	牛顿恒等式
NFS	Number Field Sieve 数域筛法
Nguyen-Regev Algorithm	Nguyen-Regev 算法
NIDS	Network Intrusion Detection System 网络入侵检测系统
Niederreiter Encryption Scheme	Niederreiter 加密方案
Nilpotent	幂零

Nilpotent Element	幂零元
NIST	National Institute of Standards and Technology（美国）国家标准技术研究所
NIZK	Non-Interactive Zero-Knowledge Proof 非交互零知识证明
NL	Nonlinearity 非线性
NLFSR	Nonlinear Feedback Shift Registers 非线性反馈移位寄存器
Node-Disjoint Path	节点不相交路径
Noiseless Database	无噪数据库
Noisy Channel	噪声信道
Noisy Correlation	噪声相关结构
Noisy Encoding	有噪编码
Noisy Factoring	噪声分解
Noisy Function	噪音函数
Noisy Leakage Model	噪声泄漏模式
Noisy Response	噪声回应
Noisy RSA Key Recovery	有噪声的 RSA 密钥恢复
Noisy Side-Channel Leakage	有噪侧信道泄漏
Noisy-Storage Mode	有噪音存储模型
No-Lone Zone（NLZ）	无单人区域，确保两人以上区域
Non-Adaptive	非自适应
Non-Adaptive Adversary	非自适应性敌手
Non-Adjacent Form	非邻接形式
Non-Aggregate ECDSA	非聚集 ECDSA（ECDSA 应当是椭圆曲线的 DSA，数字签名算法标准）
Nonassociative	非结合
Non-Black Box Manner	非黑盒方式
Non-black Box Extraction Assumption	非黑盒子抽取假设

Non-Black-Box-Way	非黑盒的方式
Non-Blind Watermarking	非盲水印
Nonce	唯一数，随机数
Nonce Length	唯一数长度
Nonce-Misuse	随机数误操作
Non-Coincidence Exhaustion	不重合穷举
Non-Commutative	非交换的
Non-Compressing Primitive	非压缩性基元
Non-Cyclic	非循环的，非周期的
Non-Degenerate	非退化的
Non-Deterministic Machine	非确定性图灵机
Non-Deterministic Random Bit Generator（NRBG）	非确定性随机比特发生器
Non-Essential	不重要的
Non-Essential Function	非本质功能，不重要的功能
Non-Extractable	非抽取的
Non-Ideal Channel	非理想信道
Non-Injective	非单射
Non-Interactive	非交互型的
Non-Interactive Assumption	非交互式假设
Non-Interactive Commitment Scheme	非交互式承诺方案
Non-Interactive Completeness Theorem	非交互完备性定理
Non-Interactive Construction	非交互式结构
Non-Interactive Proof	非交互证明
Non-Interactive Threshold Encryption	非交互性门限加密
Non-Interactive Zero-Knowledge Proof	非交互式零知识证明

Non-Interactively Complete Secure	非交互式完整安全
Non-Invasive Attack	非侵入性攻击
Non-Linear Feedback Shift Register	非线性反馈移位寄存器
Non-Linear Layer	非线性层
Non-Linear Recurrence Sequence	非线性递归序列
Non-Linearity of Boolean Function	布尔函数的非线性性
Nonlinearity Order	非线性阶
Non-Local Maintenance	非局部维护
Non-Malleability	不可延展性
Non-Malleable Code	不可锻造码
Non-Malleable Encryption	不可扩展的加密
Non-Multiplicativity	非积性
Non-Negligible Advantage	非微小优势
Non-Negligible Leakage	不可忽视的泄漏
Non-Organizational User	非组织用户，公共用户
Non-Parametric	非参数的
Nonperiodic Key	非周期性密钥
Non-Random Property	非随机特性
Non-Repudiation	不可否认性
Nonresidue	非剩余
Non-Secret Key Encryption	非私钥加密
Non-Singular Boolean Function	非奇异布尔函数
Non-Singular LFSR	非奇异线性反馈移位寄存器
Non-Tight	不紧的（指规约的紧性）

Non-Transferable	不可转让的
Non-Transferable Credential	不可转让证书
Non-Transferable Signature	不可转让签名
Non-Trivial Accuracy	有意义精确度
Non-Trivial Equation	非平凡方程
Nontrivial Finite Asymmetric Functionality	非平凡的有限非对称功能
Nontrivial Output	非平凡输出
Nonuniform Security	非均匀安全
Nonvolatile Memory	非易失性存储器
Norm	范数（数学）
Normal	正式的，标准，常态
Normal Base	正规基
Normal Base Theorem	正规基定理
Normal Profile	正常剖面
Normalize	归一化
Normalized Gaussian Integer	规范的高斯整数
Not Public Data	非公开数据
NP-Complete	NP 完全问题
NR Attack	NR 攻击
NR Gradient-Descent Attack	NR 的梯度下降攻击
N-Residue	N 次剩余
NSA-Approved Cryptography	（美国）国家安全局批准的密码
N-th Residuosity Assumption	N 次剩余假设
NTRU	Number Theory Research Unit 算法
Ntrusign Lattice	Ntrusign 格（数字签名技术）
Null	空值，零
Null Cipher	空暗码
Number Field	数域

Number Field Sieve	数域筛法
Number Theoretic Assumption	数论假设
Number Theory	数论
Number-Theoretic	数论的
Number-Theoretic Assumption	数论假设
Numerator	分母
Nyberg-Rueppel Signature Scheme	Nyberg-Rueppel 签名方案

O

O（Big-Oh）	大 O 记号
o（Small-Oh）	小 o 记号
OAEP	Optimal Asymmetric Encryption Padding 最佳非对称加密填充
Obfuscation	混淆
Object	对象
Object Identifier	对象标识符
Object Reuse	对象重用
Oblivious RAM	不经意 RAM
Oblivious Transfer（OT）	不经意传输
Oblivious Transfer（OT）Protocol	不经意传输协议
Oblivious Trusted Third Party	不经意可信第三方
Observer	观测者
OCB	Octal Coded Binary 八进编码二进数
OCSP	Online Certificate Status Protocol 在线证书状态协议，在线证书状态查询
Octonions	八元数
Odd Number	奇数
Odd Perfect Number	奇完全数
Odd-Characteristic Extension	奇数特征扩展
OEF	Origin Element Field 原点元件栏，起始单元字段
OFB	Output Feedback Block 输出反馈
Off-Card	校验器，卡外

Off-Host Processing	脱离主机处理
Official Information	官方消息
Off-Line	离线
Off-Line Attack	离线攻击
Off-Line Authentication	离线鉴别证书
Off-Line Computation	离线计算
Off-Line Credentials	离线证书
Off-Line Cryptosystem	(脱机) 离线密码系统
Off-Line Electronic Payment	离线电子支付
Off-Line Electronic Postage	离线电子邮资
Off-Line Processing	离线处理
Offset Codebook	分支编码本
Offsite	非现场
Off-Site Storage Facility	非现场存储设备
Off-the-Shelf	现成的
OFT Protocol	OFT 协议
OMA	Object Management Architecture 对象管理体系结构，物件管理架构
OMAC	Open Modular Architecture Controller 结构控制器
Omega-Notation	欧密茄记号
On-Card	卡内
One Round	一轮
One to One	一对一
One-More Forgery	一对多伪造
One-Part Code	单方码
One-Round Succinct MIP	一轮简明 MIP
One-Time Blind Signature	一次性盲签名
One-Time Cryptosystem	一次性密码系统

One-Time Key	一次性密钥
One-Time Pad	一次性填充
One-Time Password	一次性密码，一次性口令
One-Time Session Key	一次性会话密钥
One-Time Signature	一次性签名
One-Time Tape	一次性密码本
One-Way Accumulator	单向累加器
One-Way Function	单向函数
One-Way Function Tree Protocol	单向函数树协议
One-Way Group Homomorphism	单向群同态
One-Way Hash Algorithm	单向哈希算法
One-Way Hash Function (OWHF)	单向哈希函数
One-Way Permutation	单向置换
One-Way Secret-Key Agreement	单向密钥协议
One-Way Secret-Key Rate	单向密钥速率
Onion Routing	洋葱路由
Online Attack	在线攻击
OnLine Authentication Method	在线认证方法
OnLine Cam	在线中央地址存储器，在线通信存储管理器
Online Certificate Status Protocol (OCSP)	在线证书状态协议
Online Cipher	在线密码
On-Line Computation	在线计算

On-line Credential	在线的凭证
On-line Cryptosystem	在线密码系统
On-line Electronic Payment	在线电子支付
On-Line Electronic Postage	在线电子邮资
On-line Mutual Authentication	在线相互认证
On-line System	在线系统
O-Notation	大 O 记法
Onslaught	攻击
Opaque	不透明的
Open Checklist Interactive Language（OCIL）	开放清单交互式语言
Open Code	开放码，开放源代码
Open PGP	打开加密软体
Open Problem	开放问题，待解问题
Open Source	开源式
Open Storage	开放式存储
Open System Interconnection Reference Model（OSI Model）	开放系统互连参考模型
Open Vulnerability and Assessment Language（OVAL）	开放脆弱性评估语言
Open SSL	开放 SSL
Operating System（OS） Fingerprinting	操作系统指纹识别
Operating System（OS or O/S）	操作系统
Operational Control	操作控制，运行控制
Operational Key	操作密钥
Operational Vulnerability Information	操作易受到攻击信息

Operational Waiver	操作弃权
Operations Code	操作码
Operationson Dynamic Sets	动态集合操作
Operations Security (OPSEC)	操作安全
Operator	算符，算子
Opposite	对立的
Optima	最佳的
Optimal	优化的
Optimal Asymmetric Encryption Padding	最优非对称加密填充
Optimal Authentication Scheme	最优认证方案
Optimal Collision Resistance	最佳抗碰撞性
Optimal Collision Security	最优碰撞安全性
Optimal Constructions	最优结构
Optimal Extension Field	最优扩展域
Optimal Reduction	优化归约
Optimal Resiliency Condition	最理想的弹性条件
Optimal Verification	优化验证
Optimality	最优性
Optimistic Contract Signing	最优协议签署
Optimization	优化（措施）
Optimize Different Parameter	优化差分参数
Optional Modification	选择调试
Oracle	Oracle 资料库软体，预言
Oracle Access	预言抽象访问
Oracle Model	预言模型
Orange Book	橙皮书
Orbit	轨道

Order	阶，订单，排序
Order（Annihilator）	阶（零化子）
Order Isomorphism	阶同构
Order Preserving	保序的，保阶的
Orderable	按顺序的
Ordered	有序的，整齐的
Ordered Field	有序域
Order Preserving Symmetric Encryption	保序对称加密
Ordinary Curve	普通曲线
Ore's Imbedding Theorem	Ore（人名）的嵌入定理
Organization	组织，机构
Organizational Information Security Continuous Monitoring	组织信息安全持续监控
Organizational Maintenance	组织维护
Organizational Registration Authority（ORA）	组织登记机构
Organizational User	组织用户
Original Privacy	原始隐私
Original State	初态
Orthogonal	正交的，正交直线
Orthogonal and Symplectic Group	正交和辛群
Orthogonality Property	正交性
Orthonormal	正交归一化
OSI	Open System Interconnection 开放式系统互联
OS or O/S	Operating System 操作系统

OST	Operational Support Team 业务支持团队
OT	Oblivious Transfer 不经意传输
OTP	Optimal Test Procedure 最佳测试程序
Outer Mode	外模式
Outlier Behavior	异常行为
Out-of-Phase Autocorrelation	异向自相关
Output Bit	输出比特位
Output Feedback	输出反馈
Output Transformation	输出变换
Outsider Threat	外部威胁
Outsider Secure	局外人安全，不相关人安全
Outsource	外包
Outsourced Server	外包服务器
Outsourced Storage	外包存储
Outsourcing Randomness	外包随机性
Overhead	超量
Overspender Detection	过度检测
Overspending Prevention	过度预防
Overt Channel	公开信道，公开的通道，正式通道
Overt Testing	公开测试
Over-the-Air Key Distribution	无线密钥分配
Over-the-Air Key Transfer	无线密钥传递
Over-the-Air Rekeying (OTAR)	无线密钥更新
Overwrite Procedure	覆写程序
OWHF	One Way Hash Function 单向函数求逆，单向哈希函数

P

P3P	一种个人隐私安全平台（the Platform for Privacy Preferences）的标准
Packet	数据包
Packet Filter	滤包器
Packet Sniffer	数据包嗅探器
Padding	填充
Padding Oracle Attack	填充预言攻击
PAG	PKI Assessment Guidelines，PKI 评估指南（通过加密的数字签名技术为客户在法律上提供证据）
Paillier Assumption	Paillier 假设
Paillier Encryption and Signature	Paillier 加密和签名
Pairing	配对，双线性对
Pairing Computation	配对计算
Pairing Product Equation	结对生成方程
Pairing-Based Cryptography	配对密码学
Pairing Over Elliptic Curve	椭圆曲线上的配对
PAP	Password Authentication Protocol 口令认证协议
Paradigm	范式，范例
Parallel	并行
Parallel Architecture	并行架构
Parallel Composition	并行组合
Parallel Matching Algorithm	并行匹配算法

Parallelizability	并行性
Parallelized Collision Search	并行碰撞搜索
Parameter	参数
Parameterize	参数化
Parameterized Language	参数化语言
Parameterized Version	参数化的版本
Parity	奇偶性，奇偶校验位
Parity Check Matrix	奇偶校验矩阵
Parity Check Polynomial	奇偶校验多项式
Parity Check Symbol	奇偶校验符号
Parseval's Relation	巴塞夫关系（也称瑞利能量相关）
Partial Fraction	部分分式
Partial Fraction Decomposition	部分分式分解
Partial Lossiness	部分有损
Partial Preimage Resistance	部分原像计算困难性，抗部分原像
Partial Signature	部分签名
Partial-Domain One-Wayness	部分域单向性
Partially Ordered Set	偏序集
Participant Attack	参与者攻击
Particle	粒子
Partition	分割，划分
Partition Number	划分数，拆分数
Partitioned Security Mode	分区安全模式
Partitioning Cryptanalysis	分区密码分析
Party	参与方
Pascal's Triangle	帕斯卡三角形
Passive Adversary	被动攻击者
Passive Attack	被动攻击

Passive Cryptanalysis	被动密码分析
Passive Eavesdropper	被动窃听者
Passive Penetration Test	被动渗透测试，被动贯入度试验
Passive Security Testing	被动安全测试
Passive Wiretapping	被动窃听
Password	密码，口令，通行密码
Password Authenticated Key Exchange（PAKE）	口令认证密钥交换
Password Authenticated Key-Exchange Protocol	口令认证密钥交换协议
Password Complexity	口令复杂性
Password Cracking	口令破解
Passphrase	密码，通行码
Password Protected	密码保护
Pastry Dough Mixing	组成交替替换和换位
Patch	补丁
Patch Management	补丁管理
Path History	路径历史
Pattern Finding	模式查找
Pauli Operator	泡利算符
Pay Later	后付款
Pay Now	现付
Payload	有效载荷
Payment Authorization	付款授权
Payment Card	支付卡
PCI	Payment Card Industry 支付卡行业
PCP of Proximity	PCP 近似问题
PCR	Program Control Register 程序控制暂存器
P-Defect	P 亏量

Peano's Axioms	皮亚诺公理
PEAP	Protected Extended Application Protocol 受保护的扩展应用协议
Pebbling	"卵石" 算法
Peer Entity Authentication	同级实体认证
Pell-Like Equation	佩尔型方程
Pell's Equation	佩尔方程
Pell's Equation Theorem	佩尔方程定理
PEM	Privacy Enhanced Mail 增强保密邮件
Pencils of Matrices	矩阵束
Penetration	渗透
Penetration Testing	渗透测试
Pentagonal Number	五角数
PEP	Policy Enforcement Point 策略执行点
Per Multiplication	每次乘法
Per-Call Key	Per-Call 密钥
Perfect	完美的，完成式
Perfect Cryptosystem	完美保密系统
Perfect Forward Secrecy (PFS)	完美前向保密
Perfect Multiplication Protocol	完美乘法协议
Perfect Number	完全数
Perfect Security	完美安全
Perfect Threshold Scheme	完美门限方案
Perfect Zero Knowledge	完美零知识
Perfectly Secure	完美安全的
Perfectly Secure Steganography	完美安全加密
Performance Reference Model (PRM)	绩效参考模型

Perimeter	外围网络
Perimeter Security	外围安全
Perimeter Equipment	外围设备
Period Modulo M of the Fibonacci Sequence	斐波那契序列模 m 的周期
Period of a Polynomial	多项式周期
Period of a Sequence	序列周期
Periodic	周期的
Periodic Continued Fraction	周期连分数
Periodic Continued Fraction Theorem	周期连分数定理
Periodic Key	周期密钥
Periods Processing	周期处理
Perishable Data	损害数据
Permission	许可
Permitted Subtree	允许子树
Permitting Composition	允许组成
Permutation	置换，序列，排列
Permutation Matrix	置换矩阵，排列矩阵
Permutation-Based	基于置换的
Permutation-Based Mode	基于置换模式
Permute	置换（动词）
Permuted Kernel	置换内核
Permuted Perceptron	置换感知器
Permuter	置换器，换码器
Person Pseudonym	个人假名
Personal Firewall	个人防火墙
Personal Identification Number（PIN）	个人识别号码，个人密码，密码

Personal Identity Verification (PIV)	个人身份验证
Personal Identity Verification Accreditation	个人身份验证认可
Personal Identity Verification Card（PIV Card）	个人身份验证卡（PIV 卡）
Personal Identity Verification Issuer	个人身份验证发行人
Personal Identity Verification Registrar	个人身份验证注册
Personal Identity Verification Sponsor	个人身份验证赞助商
Personal Nemesis Adversary	个人复仇对手
Personal Trust Agent（PAT）	个人认证代理，个人信任管理
Personalization	个性化
Personally Identifiable Information（PII）	个人身份信息
Personnel Registration Manager	个体注册经理
Pervasive Computing	普适计算
PES	Proposed Encryption Standard 拟加密标准
Pfaffian	普法夫微分方程
PFE	Private Function Evaluation 私有函数估值
P-Frobenius Automorphism	P-Frobenius 自同构
PFS	Perfect Forward Secrecy 完全向前保密
PGP	Pretty Good Privacy 完美隐私，完美加密
P-Group	P 群
Phase Gate	相位门
Phase Noise Source	相位噪声源
Phishing	网络钓鱼

Photon	光子
Physical Attack	物理攻击
Physical Safeguard	实体防护
Physical Security	物理安全性
Physically Isolated Network	物理隔离网
Physically Unclonable	物理不可克隆
Pigeon Hole Principle	鸽笼原理
PII Confidentiality Impact Level	加密 PII 数据安全级别
Piling-Up Lemma	堆积引理
PIN	Personal Identification Number 个人身份号
PIN Verification	PIN 验证
PKCS	Public-Key Cryptography Standards 公共密钥加密标准
PKG	Private Key Generator 私钥生成器
PKI	Public Key Infrastructure 公钥基础设施
Plain Model	朴素模型
Plaintext	明文
Plaintext Awareness	明文知晓性
Plaintext Ciphertext Compromise	明文密文妥协方案
Plaintext Distinguishing Attack	明文区分攻击
Plaintext Key	明文密钥
Plaintext Compromise	明文妥协方案
Plan Activation	计划激活
Plan of Action and Milestones (POA&M)	行动和里程碑计划
Platform	平台

Platform for Privacy Preferences Project	隐私首选项平台项目
Platform Security	平台安全
Plausible Lattice-Based Construction	可靠的基于格的结构
Playback Control	回放控制
Playfair Cipher	普莱费尔密码
Plucker Coordinate	Plucker 坐标
Plucker Equation	Plucker 方程
Plug-In	插件
PMAC	PMAC 算法（由 Black and Rogaway 设计的一种消息认证码算法）
PN-Sequence	PN 序列
Pohlig-Hellman Algorithm	Pohlig-Hellman 算法
Point Addition	点加法器
Pointat Infinity	无穷远点
Point Doubling	点倍加
Point Multiplication	点乘
Polar Code	极化码
Polar Form	极化形式
Polarization	极化，偏振
Polarization Phenomenon	极化现象
Policy	政策，策略
Policy Administration Point	策略管理点
Policy Approving Authority (PAA)	政策审批管理局
Policy Certification Authority (PCA)	政策认证中心
Policy Constraint	政策约束

Policy Control	政策调控
Policy Decision Point	策略决策点
Policy Enforcement Point	策略执行点
Policy Management Authority (PMA)	策略管理机构
Policy Mapping	策略映射
Policy Mapping Inhibit Indicator	策略映射抑制指标
Policy-Based Access Control (PBAC)	基于策略的访问控制
Pollard's Kangaroo Method	Pollard 袋鼠算法
Pollard's Lambda Method	Pollard 拉姆达算法
Pollard's P-1 Method	Pollard P-1 算法
Pollard's Rho Method	Pollard Rho 算法
Polly Cracker	泼莉裂解系统
Polyalphabetic Encryption	多表加密
Polyalphabetic Substitution	多表替代
Polybios Square Encryption	Polybios 方加密
Polygraphic Substitution	多置换代替
Polylog	多对数
Polylogarithmic	多对数
Polynomial	多项式（的）
Polynomial Algebra	多项式代数
Polynomial Basis Representation	多项式基表达
Polynomial Complexity	多项式复杂性
Polynomial Equation	多项式方程
Polynomial Evaluation	多项式赋值
Polynomial Function	多项式函数

Polynomial Modulus	多项式模
Polynomial Multiplication	多项式乘法
Polynomial Security	多项式安全
Polynomial System	多项式系统
Polynomial Time	多项式时间
Polynomial-Bounded	多项式界的
Polynomially-Large Binary Circuit	多项式规模的二进制电路
Polynomial Size	多项式尺度
Polynomial Time Solution	多项式时间解决方案
Polyphony	多项式
Pontifex	Pontifex 算法
Popular	普遍存在的
Port	端口
Port Scanning	端口扫描
Portable Computing Device	便携式计算设备
Portable Media	便携式媒体设备
Porta Encryption	Porta 加密
Porta Table	Porta 表
Portable Electronic Device (PED)	便携式电子设备
Portal	门户
POS	Point of Sale 销售点终端
Position Verification	位置校验
Positive Control Material	阳性对照材料
Positive Definite	正定的
Positive Integer	正整数
Possibly Degraded Leakage Model	可能泄漏消减的模型

Post Quantum Cryptography	后量子密码学
Post-Quantum	后量子
Postal Security Device	邮件安全装置
Potential Impact	潜在影响
Potentially	可能地
Power	幂
Power Associativity	幂的结合性
Power Residue Symbol	指数剩余符号
Power Series	幂级数
Power Set	幂集
Power Trace Analysis	(网络) 功耗轨迹分析
Power Variability	指数变量
Power-of-Two Cyclotomic	2 的幂次分圆环
Powers Modulo M	幂模 M
Powers Modulo P	幂模 P
PP	Protection Profile 保护内容,保护轮廓
P-Polynomial	P 多项式
Practical Complexity	实际复杂度
Practical Four-Round Protocol	实用四轮协议
Pre-Charged Dual Rail Logic	预充电双轨逻辑
Pre-Computation Attack	预计算攻击
Pre-Computed Table	预处理表单
Precursor	前导
Predecessor	前期产品
Predecessor Attack	前驱攻击
Predicate	谓词
Predicate Encryption	谓词加密
Predicate Privacy	谓词隐私
Predictable Sequence	可预测的序列

Prediction Resistance	（确定性随机比特生成器的）抗预测性
Predisposing Condition	诱发条件
Prefix Collision	前缀碰撞
Preimage	原像
Preimage Attack	原像攻击
Preimage Resistance	抗原像性
Preimage Search	原像搜索
Preimage Security	原像安全性
Pre-Pay	预付费
Pre-Period	预期
Preproduction Model	试生产型号
Prerequisite	前提
Pre-Sampling	预取样
Pre-Specified Inputs	预先确定的输入
Pretty Good Privacy	完美隐私
PRF	Pseudo-Random Function 伪随机函数
PRF-to-PRP Conversion	PRF 向 PRP 转换
Primality Problem	素性问题
Primality Proving Algorithm	素性证明算法
Primality Test	素性测试
Primary	首要的，原始的，次素的
Primary Services Node (PRSN)	主要服务节点
Prime	素数，素的
Prime Certificate	基本证书
Prime Divisibility Property	素数整除性质
Prime Field	素域
Prime Field Anomalous Curve	素域异常曲线
Prime Generation	素数（质数）生成

Prime Number	素数，质数
Prime Number Theorem	素数定理
Prime Order	素数阶
Prime Order Field	素数阶域
Prime Order Group	素数阶群
Prime Order Setting	素数阶设置
Primitive	原函数，原语，元件，基本部件，本原的
Primitive Cyclic Code	本原循环码
Primitive Element	本原元
Primitive Element (of an Extension Field)	本原元（一个扩展域）
Primitive Polynomial	本原多项式
Primitive Pythagorean Triple	本原勾股三元组
Primitive Root	本原根
Primitive Set Operation	本原集合运算
Primitives	本原元
Primitivity (for a Group Action)	（群作用的）本原性
Principal	主要的
Principal Accrediting Authority (PAA)	主认证机构
Principal Certification Authority (CA)	主认证机构
Principal Ideal	主理想
Principal Ideal Ring	主理想环
Print Suppression	打印封锁
Priori Statistical Power Analysis	先验统计功耗分析
Privacy	隐私

Privacy Enhanced Mail	增强保密邮件
Privacy Enhancing Technology	隐私增强技术
Privacy Function	隐函数
Privacy Impact Assessment (PIA)	隐私影响评估
Privacy Issue	秘密性问题
Privacy System	隐私制度
Private Channel Coding	秘密信道编码，专用信道编码
Private Channel Model	秘密信道模型
Private Input	秘密输入
Private Key	私有密钥
Private Key Cryptosystem	对称钥密码体制
Private Key Generator	对称密钥生成器
Private Random Data	秘密随机数据
Private Set Intersection	秘密集交并
Private Watermarking	秘密水印
Privilege	特权
Privilege Management	权限管理
Privileged Account	特权账户
Privileged Command	特权命令
Privileged Process	特权进程
Privileged User	特权用户
PRNG	Pseudo Random Number Generator 伪随机数发生器
PRNG Mode	伪随机数生成器模式
Proactive Group Signature	积极的群签名
Proactive Password	主动口令
Proactive Threshold Cryptography	主动门限密码学

Proactive Threshold Signature	主动门限签名
Probabilistic	概率性的
Probabilistic Algorithm	概率算法
Probabilistic Analysis	概率分析
Probabilistic Method	概率方法
Probabilistic Primality Test	概率素性测试
Probabilistic Public Key	概率公钥
Probabilistic Signature Encryption	概率签密
Probabilistic Signature Scheme	概率签名方案
Probabilistic SSS	概率 SSS
Probabilistically-Checkable Proof	概率可检测证明
Probability	概率
Probability Density Function	概率密度函数
Probability of Occurrence	发生概率
Probable Prime	可能质数
Probe	探头
Procedural Safeguard	程序保障
Process	程序，进程
Product Cipher	乘积密码
Product Formula for Euler ϕ Function	欧拉函数 ϕ 的乘积公式
Product Rule for Indices	指标的乘积法则
Product Source Node（PSN）	产品来源节点
Production Model	产品型号
Profiling	剖析
Program	项目，程序

Programmable Hash Function	可编程散列函数
Projecting Bilinear Pairing	射影双线性对
Projection	投射，射影
Projection Map	投影映射，投影贴图
Projection Measurement	投影测量
Projective Duality	射影对偶
Projective Geometry	射影几何
Projective Orthogonal Group	射影正交群
Projective Space	射影空间
Projective Symplectic Group	射影对称群，射影酉群
Projective Unimodular	投射单模
Projective Varieties	射影簇
Promiscuous Mode	混杂模式
Proof of Security	安全性证明
Proof Sketch	证明框架
Proofs of Membership	成员证明
Propagation Criterion	扩展准则，传播准则
Property Preserving	保持性能
Property Preserving Encryption（PPENC）	保持性能的加密
Proposed Encryption Standard	所提出的加密标准
Proprietary Information（PROPIN）	专有信息
Protected Distribution System（PDS）	受保护的分布系统
Protection	保护
Protection Philosophy	防护理念
Protection Profile	保护个人资料
Protective Distribution System	防护分布系统

Protective Packaging	保护包装
Protective Technology	保护技术
Protocol	协议
Protocol Data Unit	协议数据单元
Protocol Entity	协议实体
Proton	质子
Prototype Chip	标准芯片
Provable Prime	可证素数函数
Provable Security	可证安全性
Provable Setting	可证明环境
Prove Validity	证明有效性
Prover	证明者
Provide Message Authentication	实现消息认证，供消息认证
Proving	证明
Proving Algorithm	证明算法
Provisioning	配置（文件）
Proxy	代理
Proxy Agent	代理机构
Proxy Encryption	代理加密
Proxy Server	代理服务器
Proxy Signature	代理签名
PSAM	Purchase Secure Access Module 销售点终端安全全存取模块
PSD	Phase Shift Driver 移相驱动器
PSEC-KEM	PSEC-KEM 密钥交换协议
PSEP	Probabilistic Signature Encryption Padding 概率性签名加密填充
Pseudo Deterministic	伪确定性

Pseudo Mersenne Prime	伪梅森素数
Pseudo-Hadamard Transform	伪 Hadamard 变换
Pseudo-Noise Sequence	伪噪声序列
Pseudonym	化名
Pseudonymity	假名
Pseudo-prime	伪素
Pseudorandom	伪随机性
Pseudorandom Functions (PRFS)	伪随机函数
Pseudorandom Generator	伪随机生成器
Pseudorandom Number Generator (PRNG)	伪随机数生成器
Pseudorandom Object	伪随机对象
Pseudorandom Permutation	伪随机置换
Pseudorandom Separator	伪随机分离器
Pseudorandom Sequence	伪随机序列
PSS	Probabilistic Signature Scheme 概率签名方案
PSS-R	PSS 的改进方案，可提供信息恢复的概率签名方案
Public Domain Software	共享软件
Public Index	公开指标
Public Key	公钥，公开密钥
Public Key (Asymmetric) Cryptographic Algorithm	公钥（非对称）加密算法
Public Key Based Protocol	基于公钥的协议
Public Key Certificate	公钥证明书
Public Key Compression	公钥压缩
Public Key Cryptosystem	公钥密码系统

Public Key Cryptography	公钥密码学
Public Key Cryptography Standard	公钥加密标准
Public Key Enabling (PKE)	公钥启用
Public Key Encryption	公钥加密
Public Key EncryptionScheme	公钥加密方案
Public Key Infrastructure (PKI)	公钥基础设施
Public Key Proxy Encryption	公钥代理加密
Public Key Proxy Signature	公钥代理签名
Public Key Setting	公钥设置
Public Key Stegosystem	公钥隐秘系统
Public Key Watermarking	公钥水印
Public Parameter	公共参数
Public Permutation	公开置换，公开排列
Public Seed	公开种子（密钥）
Public Source of Randomness	公开的随机源
Public Verifiability	公开可验证性
Public Watermarking	公开水印
Publicly Verifiable Secret Sharing	公开可验证秘密共享
Purchase Secure Application Module	购买安全应用模块
Pure Circulating Register	纯循环寄存器
Pure Cryptosystem	纯密码系统
Purely Periodic Continued Fraction	纯周期连分数
Purge	清除
Purification	纯化

Purse	钱包
Pythagpras Hypotenuse Proposition	毕达哥拉斯斜边命题
Pythagpras Theorem	毕达哥拉斯定理
Pythagpras Triangle	毕达哥拉斯三角形
Pythagpras Triple	勾股数组

Q

Quantitative	定量的，定性的
QC-Extractor	QC 提取器
Q-Curve	Q 曲线
Q-Matrix	Q 矩阵
QOS	Quality of Service 服务质量
Q-Query	查询
QS	Quadratic Sieve 二次筛法（指简化数学难题的方法）
Quadrant	象限（四分之一圆周）
Quadratic	二次的
Quadratic Complexity	二次复杂性
Quadratic Equation Modulo	二次方程模
Quadratic Extension	二次扩张
Quadratic Form	二次形式，二次型，二次齐次多项式
Quadratic Frobenius Test	二次 Frobenius 测试
Quadratic Function	二次函数
Quadratic Nonresidue	二次非剩余
Quadratic Reciprocity Law	二次互反律
Quadratic Residue	二次剩余
Quadratic Residuosity	二次剩余
Quadratic Residuosity Assumption	二次剩余假设
Quadratic Residuosity Problem	二次剩余问题
Quadratic Sieve	两次筛法（指简化数学难题的方法）
Quadratic Span Program	二次跨度程序

Quadratic Time	二次时间
Quadratic Time Algorithm	二次时间算法
Quadratical	二次方的
Qualitative Assessment	质量评定
Qualitative Difference	质量差异
Quantitative Assessment	定量评定
Quantitative Connection	量化关系
Quantitative Security Bound	定量安全边界
Quantum	量子
Quantum Adversary	量子敌手
Quantum Algorithm	量子算法
Quantum Attack	量子攻击
Quantum Bit Commitment (QBC)	量子比特承诺
Quantum Channel	量子信道
Quantum Coin Flipping (QCF)	量子掷币
Quantum Communication	量子通信
Quantum Computer	量子计算机
Quantum Cryptography	量子密码学
Quantum Entanglement	量子纠缠
Quantum Key Agreement (QKA)	量子密钥协商
Quantum Key Distribution (QKD)	量子密钥分配
Quantum Measurement	量子测量
Quantum Mechanics	量子力学
Quantum Memory	量子存储器
Quantum Oblivious Transfer (QOT)	量子不经意传输

Quantum Optics	量子光学
Quantum Oracle Model (QROM)	量子随机预言模型
Quantum Private Comparison (QPC)	量子保密比较
Quantum Proof of Knowledge	量子知识证明
Quantum Random	量子随机
Quantum Rewinding Technique	量子复放技术
Quantum Secret Sharing (QSS)	量子密钥共享
Quantum Secure Direct Communication (QSDC)	量子安全直接通信
Quantum Secure Multiparty Computation (QSMPC)	量子安全多方计算
Quantum Setting	量子条件
Quantum Side Information	量子侧信息
Quantum Signature (QS)	量子签名
Quantum State	量子态
Quantum Teleportation (QT)	量子隐形传态
Quantum to Classical	量子至经典的
Quantum Zero-Knowledge	量子零知识
Quantum-Immune Identification Scheme	量子免疫识别方案
Quantum-Immune Signature Scheme	量子免疫签名方案
Quarantine	隔离
Quartet	四进制
Quartet Constraint	四元组约束
Quasi Knowledge	准知识

Quasi-Adaptive	近似自适应
Quasi-Invertible Element	拟可逆元
Quasi-Polynomial	拟多项式
Quasi-Polynomial Approximation Factor	拟多项式近似因子
Quaternary Alphabet	四进制字母表
Quaternion	四元数
Qubit	量子比特，量子位
Qubit Efficiency	量子比特效率
Query	查询
Query Complexity	查询复杂性
Quick Mode IPSec	快速模式网际协议安全
Quotient	商
Quotient Lattice	商格
Quotient Module	商模
Quotient Ring	商环

R

Registration Authority（RA）	注册中心
Rabbit Problem	兔子问题
Rabin Cryptosystem	拉宾密码
Rabin Digital Signature Scheme	拉宾数字签名方案
Rabin's Primality Test	拉宾素性测试
Rabin-Miller Test	拉宾米勒测试
Rabin-Miller Testfor Primality	拉宾米勒素数测试
Radical	自由基，根本的，根式
Radically Different	完全不同
Radio Frequency Attack	射频攻击
Radio Frequency Identification（RFID）	无线射频识别技术
RADIUS	Remote Authentication Dial In User Service 远程认证拨号用户服务
Rainbow Table	彩虹表
Ramified Prime	分歧素数
Ramp Scheme	Ramp 方案
Random Bit	随机位
Random Bit Generation（Hardware）	随机比特生成（硬件）
Random Bit Generator（RBG）	随机位发生器
Random Coding Technique	随机编码技术
Random Key	随机密钥

Random Linear Code	随机线性码
Random Message Attack	随机消息攻击
Random Number Generator (RNGS)	随机数发生器
Random Oracle	随机预言
Random Oracle Model	随机预言模型
Random Order-Preserving Function	随机保序函数
Random Permutation Model	随机置换模式
Random Preimage Attack	随机的原像攻击
Random Projection	随机射影
Random Sequence	随机序列
Random Squares Method	随机平方算法
Random Start Index	随机开始索引
Random Tape	随机带
Randomized Algorithm	随机算法
Randomized Cascade	随机级联
Randomized Encoding	随机编码
Randomized Encryption	随机加密
Randomized Functionality	随机函数
Randomized Iterate	随机迭代
Randomized Public-Key Encryption	随机公钥加密
Randomizer	随机性发生器
Randomness	随机性
Randomness Expansion	随机性扩展
Randomness Extraction	随机提取
Randomness Extractor	随机性提取器

Randomness Postulates of Golomb	戈洛姆随机性假设
Randomness Source	随机源
Range Query	范围查询
Rank Metric	秩度量
Rank Problem	秩问题
Rational	有理数
Rational Canonical Form	有理标准形
Rational Canonical Form (or Matrix)	有理标准形（或矩阵）
Rational Function	有理函数
Rational Number	有理数
Rational Player	理性参与者
Rational Point	有理点
Rational Solution	有理数解
RBAC	Role-Based Access Control 基于角色的访问控制
RC2	RC2 加密算法
RC4	RC4 加密算法
RC5	RC5 加密算法
RC6	RC6 加密算法
Reactive Defense Password	激活防守口令
Read Access	读取
Real Closed	实封闭的
Real Closed Field	实闭域
Real Division Algebra	实可除代数
Real Execution	实际执行
Real Function	实函数
Real Number	实数

Real Time Attack	实时攻击
Real Time Reaction	实时反应
Reasonable Measure	合理措施
Reasoning Pattern	推理模式
Rebound Attack	反弹攻击
Receipt-Free Problem	无接收问题
Receiver	接收器，接收机，接收者
Receiver Deniable	收件方可拒绝的
Receiver Deniable Encryption	接收者否定加密
Recipient Anonymity	接收者匿名性
Recipient Unobservability	接收者不可观测性
Recipient Usage Period	收件人使用期限
Reciprocal Agreement	互惠协议
Reciprocity	互反律
Record	记录
Record Layer	记录层
Record Management	记录管理
Record Retention	记录保留
Recovery Point Objective	恢复点目标
Recovery Procedures	恢复过程
Recovery Strategy	恢复策略
Recovery Time Objective	恢复时间目标
Rectangle	矩形
Rectangle Attack	矩形攻击
Rectangle/Boomerang Approach	矩形/回旋镖攻击（方法）
Recursion Theorem	递归定理
Recursive Formula	递推公式

Red/Black Concept	红色/黑色概念
Reduce To	规约为
Reduced Density Operator	约化密度算子
Reduced SHA-256	缩减轮数的 SHA-256
Reduced-Round	缩减轮数
Reducible Polynomial	既约多项式
Reduction	规约
Reduction Mode	化简模式
Reductionist	规约主义者
Redundancy	冗余度
Redundantly	冗余地
Reed-Muller Code	里德缪勒码（RM 码）
Reed-Solomon Code	里德所罗门码（RS 码）
Re-Encrypt	重新加密
Reference Monitor	基准监视器
Reflection Group	反射群
Registration	注册
Registration Authority (RA)	注册机构
Regular Languages	规则语言
Regular One-Way Function	规则单向函数
Rejection Sampling Algorithm	拒绝抽样算法
Rekey (a Certificate)	更新密钥（证书）
Related Key	相关密钥
Related Key Attack	相关密钥攻击
Related-Key Rectangle Attack	相关密钥矩阵攻击
Relation (Binary)	关系（二进制）
Relationship Anonymity	关系匿名
Relationship Pseudonym	关系假名
Relatively Prime	互质，互素

Relativistic Protocol	相对论协议
Relaxed Condition	放宽松的条件
Relay Attack	中继攻击
Release Prefix	前缀附加
Reliability	可靠性
Reliable Communication	可靠通信
Reliable Erasure	可靠擦除
Relinearization	重复线性化
Relying Party	依赖方
Remainder Theorem	剩余定理
Remanence	剩磁，剩余
Remediation	整治，补救，修复
Remediation Plan	修复计划
Remote Access	远程访问
Remote Channel Extension	远程信道扩展
Remote DASD Mirroring	远程磁盘驱动器数据复制
Remote Diagnostics/Maintenance	远程诊断/维护
Remote DOS Attack	远程 DOS 攻击
Remote Maintenance	远程维护
Remote Rekeying	远程密钥更新
Remote Site	远程站点
Removable Media	可移动媒体
Renew (a Certificate)	更新（证书）
Repair Action	修复操作
Repeated Key	重复密钥
Replay Attack	重放攻击
Repository	资料库，资源库
Representation	表示

Representation (Lambda)	拉姆达表达式
Representation as Sum of Two Squares	表成两平方数之和
Representation Technique	表示技术
Representation	代表
Request for Comment (RFC)	请求评议
Re-Randomizable	重随机化的
Re-Randomize	再随机化
Reseedable Pseudorandom Sequence Generation	可重播伪随机序列生成
Reserve Keying Material	储备密钥材料
Resettable Zero Knowledge	可重置零知识
Residual Risk	剩余风险
Residue	剩余
Residue Class	剩余类
Residues Modulo an Integer	模整数剩余
Resilience	(密钥泄漏) 安全性，弹性
Resiliency Order	(代数免疫阶的) 弹性次数
Resilient	弹性的
Resource Encapsulation	资源封装
Responder	应答器，响应器
Response	回应
Responsibility to Provide	(信息发布的) 负责提供
Responsible Individual	负责人制度
Restricted	限制的
Restricted Circuit Class	约束电路类
Restricted Commitment	受限承诺
Restricted Data	(美国的) 未解密的涉密资料
Restriction Homomorphism	限制同态

Resultant	结式
Resulting Ciphertext	生成密文
Resynchronization Attack	同步攻击
Retail	Retail 密钥（附于零售光盘之上的“密钥”）
Retention Period	保留期限
Retrievability	可恢复性
Retrieval	恢复（检索）
Reusable	可重用的
Reusable Extractor	可复用抽取器
Reverse Engineering	反向工程
Reversed Alphabet	颠倒字母表
Reversible	可逆的
Revocable Credential	撤销证书
Revocation	撤销
Revocation Cryptosystem	唤回加密系统
Revocation Scheme	撤销计划
Revoke a Certificate	吊销证书
Revoked User	被取消的用户
Rewinding-Based	基于重卷的
RF Attack	射频攻击
RFID	Radio Frequency Identification Devices 无线射频识别
Rights Management	权限管理
Right-to-Left Exponentiation	从右到左求幂
Rigorous	精确的
Rigorous Proof	严格证明
Rijndael	Rijndael 分组密码算法
Ring	环
Ring Homomorphism	环同态

Ring-LWE	环上 LWE（Learning with Error）伴错学习问题
Ring-LWE Cryptography	环 LWE（Learning with Error）密码学
Ring-Switching	环转换
RIPE	Race Integrity Primitives Evaluation Race 完整性原始评价
RIPEMD Family	（哈希）函数族
Risk	风险
Risk Acceptance	风险接受
Risk-Adaptable Access Control（RADAC）	风险适应性强访问控制
Risk Analysis	风险分析
Risk Assessment	风险评估
Risk Assessment Methodology	风险评估方法
Risk Assessment Report	风险评估报告
Risk Assessor	风险评估师
Risk Assumption	风险承担
Risk Avoidance	风险规避
Risk Communication	风险沟通
Risk Estimation	风险评估
Risk Executive（or Risk Executive Function）	风险执行（或风险执行功能）
Risk Exposure	风险暴露
Risk Management	风险管理
Risk Management Framework	风险管理框架
Risk Mitigation	风险缓解
Risk Model	风险模型
Risk Monitoring	风险监控
Risk Reduction	风险降低

Risk Response	风险应对
Risk Response Measure	风险应对措施
Risk Retention	风险保留
Risk Threshold	风险阈值
Risk Tolerance	风险容忍度
Risk Transference	风险转移
RMAC	Routing-enhanced Medium Access Control 一种介质访问控制协议
Robust	鲁棒性
Robust Coin Flipping	鲁棒掷硬币
Robust Secret Sharing	鲁棒秘密共享
Robust Security Network (RSN)	强安全网络
Robust Security Network Association (RSNA)	强安全网络协会
Robustness	鲁棒性
Rogue Device	恶意设备
Rohrbach's Maxim	Rohrbach 规则
Role	角色
Role Hierarchy	角色层次
Role-Based Access Control (RBAC)	基于角色的访问控制
Root	根
Root CA	根签证机构，最高层认证中心
Root Cause Analysis	根原因分析
Root Certification Authority	根权威认证
Rootkit	隐匿技术，隐匿程式
Root Tower	根塔
Rotation	旋转

Rotor	转轮密码
Round	循环，轮数
Round Complexity	轮复杂度
Round Constant	轮常数
Round Function	轮函数
Round Key	轮密钥
Round-Optimal	轮数最优的
Round-Optimal Zero Knowledge	轮数最优零知识
Round-Reduced AES Attack	减少轮的 AES 攻击
Rounds of the Cryptosystem	密码系统的轮数
RP	Relying Party 依赖方
RPO	Recovery Point Objective 目标恢复点
RSA	RSA 公钥加密算法
RS Code	RS 码
RSAAssumption	RSA 假设
RSA Cryptosystem	RSA 公钥加密算法
RSA Digital Signature Scheme	RSA 数字签名方案
RSA Encryption	RSA 公钥加密
RSA Factoring Challenge	RSA 密码破译比赛
RSA Number	RSA 数
RSA Problem	RSA 问题
RSA Public-Key Encryption	RSA 公钥加密
RSA-CRT	RSA 与中国剩余定理（CRT = Chinese Remainder Theorem）
RSA-KEM	RSA-KEM 算法
RSA-PSS	RSA-PSS 数字签名算法
RTO	Recovery Time Objective 恢复时间目标
Rubik's Cube	Rubik 魔方

Ruffini-Abel Theorem	Ruffini-Abel 定理
Rule Book	规则书
Rule Set	规则集
Rule-Based Security Policy	基于规则的安全策略
Rules of Engagement（ROE）	交战规则
Run	运行，游程
Run Property	游程特性
Running Time	运行时间
Running-Key	运行密钥

S

S/MIME	Secure/Multipurpose Internet Mail Extensions 多用途网际邮件扩充协议
SA	Select Address 选择地址，Systems Analyst 系统分析员
SAC	Semi-Automatic Coding 半自动编码
SAEP +	博纳提出的一种非对称加密填充
Safe Prime	安全素数
Safeguard Selection	保障选择
Safeguarding Statement	防护声明
Safeguard	防范措施，安全措施，安全设备
Sally	突击，出击
Salvage Procedure	修复程序
Salvage & Restoration	救助和恢复
SAML	Security Assertion Markup Language 安全断言置标语言
Sample Distribution	样本分布
SAN	Storage Area Networking 存储器域网
Sandbox	沙盒，沙箱
Sanitization	净化政策，卫生处理
Sanity Check	完整性检查
Satoh's Algorithm	佐藤算法
Saturation Attack	饱和攻击
S-Box	S 盒
SCADA	Supervisory Control And Data Acquisition 监控和数据采集，数据采集与监控

Scalable GKE	可扩展的 GKE
Scalar Multiplication	纯量乘法，标量乘法
Scale Invariant	尺度不变
Scanning	扫描
Scanning Electron Microscope	扫描式电子显微镜
Scatter Net	分散网
Scavenging	清扫，清除
Scheme	机制，方案，概型
Schmidt Decomposition	施密特分解
Schnorr Digital Signature Scheme	施诺尔数字签名方案
Schnorr Identification	施诺尔身份认证
Schoof's Algorithm	斯格夫算法
Schroder Bernstein Theorem	施罗德伯恩斯坦定理
Schur's Lemma	舒尔引理
SDA	Symbolic Disk Address 符号磁盘地址，Source Data Automation 源数据自动化
SDMI	Secure Digital Music Initiative 安全数字音乐保护协议
SDSI	Shared Data Set Integrity 共享资料集完整性
SDSI Name	SDSI 名字
Seal	印章
Second Preimage Resistance	抗第二原像性
Second-Order Differential Collision	二阶差分碰撞
Secrecy	保密性，机密性
Secrecy Capacity	保密能力
Secret Input	秘密输入

Secret Key	秘密钥，私钥
Secret Key (Symmetric) Cryptographic Algorithm	对称密码算法
Secret Key Cryptosystem	对称钥加密系统
Secret Key Establishment	秘密密钥建立
Secret Seed	（密钥）私钥种子
Secret Sharing	秘密分享
Secret Sharing Scheme	秘密分享方案
Secretive Defense Password	秘密防御口令
Secure Authentication	安全认证
Secure Channel	安全信道
Secure Commitment	安全承诺
Secure Communication	安全通信
Secure Communication Protocol	安全通信协议
Secure Computation	安全计算
Secure Computation Protocol	安全计算协议
Secure Cryptosystem	安全密码系统
Secure Database Commitment	安全数据库承诺
Secure Digital Music Initiative	安全数字音乐促进组织
Secure DNS (SECDNS)	安全域名服务器
Secure Electronic Transaction	安全电子交易协议
Secure Erase	安全清除
Secure Erasure	安全擦除
Secure Function Evaluation	安全功能评估
Secure Hash Algorithm (SHA)	安全散列算法，安全哈希算法
Secure Hash Standard	安全散列标准
Secure HTTP	安全超文本传输协议
Secure ID	安全卡，安全码，安全标志符

Secure Multiparty Computation	安全多方计算
Secure Outsourcing	安全外源
Secure Protocol	安全协议
Secure Scheme	安全方案
Secure Shell	受限 Shell，安全壳
Secure Signatures from the “Strong RSA” Assumption	来自强 RSA 假设的安全签名
Secure Sketch	安全梗概
Secure Socket Layer（SSL）	安全套接层协议
Secure State	安全状态
Secure Subsystem	安全子系统
Secure Two-Party Computation	安全双方计算
Secure/Multipurpose Internet Mail Extensions（S/MIME）	安全多用途 Internet 邮件扩展
Security	安全性，安全
Security Against Function	安全对立函数
Security Analysis	安全性分析
Security Architecture	安全架构
Security Assertion Markup Language（SAML）	安全判定标示语言
Security Assessment	安全性评估
Security Association	安全联盟
Security Association Database	安全关联数据库
Security Attribute	安全属性
Security Authorization（to Operate）	安全授权（操作）
Security Authorization Boundary	安全授权边界

Security Automation Domain	安全自动化域名，安全自动化域名注册，安全自动化领域
Security Awareness	安全意识
Security Awareness Program	信息安全意识规划
Security Banner	安全标语
Security Bound	安全性界
Security Boundary	安全边界
Security Categorization	安全类别，安全需求分类
Security Category	安全（范畴）分类
Security Concept of Operations（Security CONOP）	安全操作概念
Security Content Automation Protocol（SCAP）	安全内容自动化协议
Security Control	安全控制
Security Control Assessment	安全控制措施评监
Security Control Assessor	安全控制评估者
Security Control Baseline	安全控制基线
Security Control Effectiveness	安全控制有效性
Security Control Enhancement	安全控制增强
Security Control Inheritance	安全控制继承
Security Domain	安全域
Security Enabled	具备安全性能的
Security Engineering	安全工程
Security Evaluation	安全评估
Security Evaluation Criteria	安全评估标准
Security Event	安全事件
Security Fault Analysis（SFA）	安全故障分析
Security Features Users Guide（SFUG）	安全特性用户指南

Security Filter	安全过滤
Security Function	安全函数
Security Gateway	安全网关
Security Goal	安全目标
Security Impact Analysis	安全影响分析
Security Incident	安全事件
Security Information and Event Management (SIEM) Tool	安全信息事件管理工具
Security Inspection	安全检验
Security Kernel	安全核心
Security Label	安全标签
Security Level	安全等级
Security Management Dashboard	安全管理仪表板
Security Margin	安全边际
Security Marking	安全标记，安全印记
Security Mechanism	安全机制
Security Module	安全管理模块，安全模块
Security Net Control Station	安全网络控制台
Security Notion	安全概念
Security Objective	安全目的
Security Parameter	安全参数
Security Parameter Index	安全参数索引
Security Perimeter	安全周边，安全界限
Security Plan	安全方案
Security Policy	安全策略，安全政策
Security Policy Database	安全策略数据库
Security Posture	安全态势
Security Procedure	安全程序

Security Program Plan	安全计划
Security Proof	安全证明
Security Range	安全范围
Security Reduction	安全性归约
Security Requirement	安全需求
Security Requirement Baseline	安全需求基线
Security Requirement Traceability	安全需求可跟踪性
Security Safeguard	安全保卫
Security Service	安全服务
Security Specification	安全性规范
Security Standard Activity	安全标准活动
Security Strength	安全强度
Security System	安全系统
Security Tag	安全标签
Security Target	安全目标
Security Test & Evaluate (ST&E)	安全系统测试与评估
Security Testing	安全测试
Security Token	安全令牌
Security Vulnerability	安全漏洞
Security-Proof Technique	安全证明技术
Security-Relevant Change	安全相关变化
Security-Relevant Event	安全相关事件
Security-Relevant Information	安全相关信息
Seed	种子
Seed Key	种子密钥
Seed-Dependent Distribution	依赖种子的分布
Seeding Random Number Generator	种子随机数发生器

Segregation of Duty	职责划分
Seidenberg's Decision Method	赛登伯格的决策方法
Selective Forgery	选择性伪造
Selective Opening	选择性开放
Selective Opening Attack	选择性开放攻击
Selective Opening Security	选择性开放安全
Self-Adjoint	自伴的
Self-Initializing Quadratic Sieve	自行初始化二次筛
Self-Reciprocal Permutation	自反置换
Self-Reducibility	自可约性
Self-Shrinking Generator	自缩减生成器
Self-Synchronizing Stream Cipher	自同步流密码
Self-Updatable Encryption	自主更新加密
SEM	Search Engine Marketing 搜索引擎营销
SEMA	Smart Embedded Management Agent 智能嵌入式管理平台
Semagram	语义编码
Semantic Security	语义安全
Semantically Secure	语义安全的
Semi-Constant Distribution	半常数分布
Semi-Direct Product	半直积
Semi-Free Start	半自由初始值的
Semi-Free-Start Collision	半自由初始值的碰撞
Semigroup	半群
Semi-Honest	半诚信/半诚实
Semi-Honest Adversary	半诚实对手
Semi-Honest Oblivious Transfer Protocol	半诚实不经意传输协议

Semi-Honest OT Protocol	半诚实不经意传输协议
Semi-Linear	半线性的
Semi-Modular	半模
Semi-Quantitative Assessment	半定量估值
Semi-Stable	半稳定
Semi-Weak Key	半弱密钥
Sender	发送者
Sender Anonymity	发送者匿名性
Sender Deniable Encryption	发送者可否认的加密
Senior Agency Information Security Officer (SAISO)	高级机构信息安全官
Senior Information Security Officer	高级信息安全官
Sensitive Compartmented Information (SCI)	敏感隔绝情报信息
Sensitive Compartmented Information Facility (SCIF)	敏感隔绝情报设施
Sensitive Information	敏感信息
Sensitive Intermediate Variable	敏感中间变量
Sensitivity	敏感性
Sensitivity Label	敏感度标签
Sensitivity Level	敏感等级
Sensor	传感器
Sensor Module	传感器模块
Separable	可分离的
Separation of Duty	职责划分
Sequences	序列
Sequential Aggregate Signature	顺序聚合签名

Sequential Aggregate Signature Scheme	顺序聚合签名方案
Sequential Composition	顺序合成，顺序成分
Sequential Execution	顺序执行
Sequentially Rational Way	序列理性方式
Sequentially Unstable	序列不稳定
Serial	串行
Series	系列，级数
Serpent	Serpent 分组密码算法
Server	服务器
Server Hello	服务器问候消息
Service	服务
Service Account	服务账户
Service Bureau	服务处，服务局
Service-Level Agreement	服务级协议
Session Key	会话密钥
Session Pseudonym	会话假名
SET	Secure Electronic Transaction 安全电子交易协议
Set of Utilities	组件集合
Set Operation	集合操作
Set-Operation Query	集合操作查询
Set-Operation Verification	集合操作验证
Setting	环境
S-Expression	S 表达式
S-Flash	串行闪存，独立型串列式快闪记忆体
SGEMP	System Generated Electromagnetic Pulse 电磁脉冲，系统电磁脉冲
Shadow Database	影子数据库

SHA Family (Secure Hash Algorithm)	SHA 族（安全散列算法）
SHA-3 Competition	SHA-3 竞选
SHACAL	SHACAL 哈希算法
Shamir's Threshold Scheme	沙米尔的门限方案
Shamir's Ultimate Knapsack Scheme	沙米尔的最终背包方案
Shamir-Zippel Scheme	Shamir-Zippel 方案
Shank's Baby-Step Giant-Step Method	尚克的小步大步方法
Shannon Theory	香农理论
Shannon's Main Theorem	香农的主要定理
Shannon's Maxim	香农原则
Shannon's Model	香农模型
Share	共享
Share Size	份额尺度
Shared Encryption Key	共享加密密钥
Shared Input	共享输入
Shared Secret	共享秘密
Shared Value	共享秘密值
Shared Variable	共享变量
Sharing Rule	共享法则
Shark	鲨，一种加密算法
Shawe-Taylor's Algorithm	沙维—泰勒算法
Shielded Enclosure	屏蔽外壳，屏蔽室
Shift Cipher	移位密码
Shift Register Sequence	移位寄存器序列
Shift-and-Add Property	移位可加性
Shifted Alphabet	移位字母

Short Digital Signature	短数字签名
Short Exponent	短指数
Short Integer Solution (SIS)	小整数解
Short Signature	短签名
Short Tag	短标签
Short Title	短标题
Shortcut Attack	捷径攻击，有效攻击
Shorter Public Key	较短公钥
Shortest Vector Problem	最短向量问题
Shrink	收缩
Shrinking Generator	缩减生成器
Shuffle	洗牌，置乱
Shuffle of Homomorphic Encryption	同态加密置乱
Shuffling Algorithm	洗牌算法
Shuffling Procedure	倒换程序
Side Channel	侧信道
Side Channel Leakage	侧信道泄漏
Side-Channel Analysis	侧信道分析
Side-Channel Analysis for Reverse Engineering (SCARE)	逆向工程的侧信道分析
Side-Channel Attack	侧信道攻击
Side-Channel Leakage	侧信道泄漏
Side-Channel Protection	侧信道保护
Siegel's Theorem	西格尔定理
Siegenthaler	西根塔勒
SIEM	Security Information and Event Management 安全信息与事件管理
Sieve of Eratosthenes	厄拉多塞筛

Sieve-in-the-Middle	中间筛
Sieving	筛分，筛选
Sieving in Function Field	函数域筛法
Sieving Technique	筛技术
Sigaba	美国的一种密码机
Sigmyc	Sigaba 密码机的前身
Sign Function	符号函数
Signature	签名
Signature Analogue	签名类比物
Signature Certificate	签名证书
Signature Class	签名类
Signature Generation	签名生成
Signature Query	签名查询
Signature Scheme without Random Oracle	无随机预言签名方案
Signature Scheme	签名方案
Signature Validation	签名确认
Signature Verification	签名验证
Signcryption	签密
Signed Data	被签名数据
Signed Data Set	被签数据集
Signed Digit Exponentiation	被签数字求幂运算
Signer's Security	签名者的安全
Signing Algorithm	签名算法
Signing Key	签名密钥
Signing Messages of Arbitrary Length	具有恒定大小的公钥（对任意长消息进行签名）
SIH	Security Intelligence Hub 安全情报中心
Simple Distributed Security	简单分布式安全

Simple Electromagnetic Analysis	简单电磁分析
Simple Group	单群
Simple Mail Transport Protocol	简单邮件传输协议，单邮件传输协议
Simple Power Analysis	简单功耗分析
Simple Public Key Infrastructure	简单公钥基础设施
Simple Ring	单环
Simple Substitution	简单替换
Simplified Asymmetric Encryption Padding	简化的非对称加密填充
Simplified Version of Shuffling	扰乱的简化版
Simulatable Encryption	冒充加密
Simulation	模拟
Simulation-Based	基于仿真的
Simulation-Sound	模拟正确性
Simulation-Sound Extractability	模拟正确可提取性
Simulation Test	仿真试验
Simulator	模拟者
Simultaneous Congruence	同余式组
Simultaneous Exponentiation	同时求幂运算
Simultaneous Security	同时安全
Simultaneous Sliding Window Exponentiation	同时滑动窗口求幂运算
Single Discrete Logarithm Algorithm	单一离散对数算法
Single Key	单密钥

Single Length Key	单长度密钥
Single Length Key Space	单长度密钥空间
Single Point Keying	单点控
Single Prover	单个证明者
Single Sign-On	单点登录
Single-Hop Problem	单跳问题
Single-Instance (SI) Security	单实例安全
Single-Key Attack	单密钥攻击
Single-Pass Authenticated Encryption	单次认证加密
Singleton Bound	辛格顿界限
Single-User Setting	单用户设置
Situational Awareness	态势感知
Size	大小，容量，尺寸
Size-Hiding	尺寸隐藏
Skew	斜
Skew Element	斜交单元
Skipjack	Skipjack 加密法
Sky Videocrypt System	星空电视加密系统
Slice	片
Slid Pair	滑动对
Slide Attack	滑动攻击
Slide with a Twist	扭曲滑动
Sliding Window Exponentiation	滑动窗口求幂运算
SLN	直线折旧法函数
Slow Key-Schedule	缓慢密钥编排
Small Embedded Device	小型嵌入式设备
Small Field	小域
Small Message	小信息

Small Polynomial	小的多项式
Small Set	小集/小参数
Small-Depth Circuit	小深度电路
Smart Card	智能存储卡
Smartcard Tamper Resistance	智能卡抗破坏性
SME	Subject Matter Expert 主题问题专家
Smooth Hash Proof System	光滑散列证明系统
Smooth Number	光滑数
Smooth Polynomial	光滑多项式
Smooth Projective Hash Functions (SPHFS)	光滑的投影哈希函数
Smoothness	平滑，光滑性
Smoothness Probability	平滑概率
SMT Solver	SMT 解题器
SMTP	Simple Mail Transfer Protocol 简单邮件传输协议
SNFS	Special Number Field Sieve 特殊数域筛法
Sniffer	嗅探器
Sniffing	嗅探，探查法
Snort	网络入侵检测系统，嗅探
Social Engineering	社会工程
Software	软件
Software Assurance	软件保证
Software Attack	软件攻击
Software Implementation	软件实现
Software System Test and Evaluation Process	软件系统测试和评价过程
Software-Based Fault Isolation	基于软件的故障隔离
Solitaire	纸牌

Solovay & Strassen's Primality Test	Solovay 和 Strassen 的素性测试
Solution Modulo P	模 p 的解
Solvability of an Equation by Radical	方程的根式可解性
Solvable	可以解的，可以解决的，可解
Solver	解算器
Somewhat Homomorphic	近似同态，有些同态性
Somewhat Homomorphic Encryption	近似同态加密
Sophie Germain Prime	索菲·热尔曼质数，索菲·热尔曼素数
Sophisticated Attack	复杂攻击
Sound Engineering Practice	可靠的工程实践
Soundness	合理性，可靠性，完整性，正确性
SP Network	SP 网络
SPA	Scratch Pad Area 暂存记忆体区
Space Bounded Computation	空间有限的计算
Space-Bounded Leakage	限域性泄漏
Spam	垃圾邮件，垃圾信息
Spam Filtering Software	垃圾邮件过滤软件
Span Program	跨度程序
SPD	Surge Protective Devices 电涌保护器
Special Access Program (SAP)	特殊访问权限程序
Special Access Program Facility (SAPF)	特殊访问程序设施
Special Character	特殊字符
Special NFS	特殊网络文件系统
Special Purpose Primality Test	特殊目的素性测试
Specification	规格，说明书，规范

Specified Bias	指定偏置
Specious Adversaries	假冒敌手
Spectral Graph	光谱图像
Spillage	溢出，溢出量
Spin	自旋
SPKI/SDSI	Simple Public Key Infrastructure/Shared Data Set Integrity 简单公钥基础设施/共享数据集完整性
Split Knowledge	分割知识
Split Prime	分裂素数
Split-State Leakage	分裂状态泄漏
Split-State Model	分裂状态模型
Splitting	分裂
SPN	Service Provider Network 业务提供者网络
SPN Paradigm	业务提供者网络（SPN）范例
Sponge Construction	海绵结构
Sponge-Like Construction	类海绵结构
Spoofing	欺骗，电子欺骗
Spread Spectrum	扩频，扩展频普
Spyware	间谍软件
SQL	Structured Query Language 结构化查询语言
Square Attack	平方攻击
Square Number	平方数
Square Root	平方根
Square Root Tower	平方根塔
Square-and-Multiply Algorithm	平方和乘法算法
Square-Root Bound	平方根界
Square-Triangular Number	三角平方数

Squaring Formula	平方公式
Squash	挤压
Squashing	压片
SSH	Secure Shell 一种用于远端登录的网络协议
SSL	Secure Sockets Layer 安全套接层
SSL Protocol	安全套接层协议
Stabilizer	稳定器
Stage	阶段
Stand-Alone Processing	独立处理
Stand-Alone Setting	独立设置
Standard	标准
Standard Alphabet	标准字母
Standard Assumption	标准假设
Standard Complexity Theoretic Assumption	标准的复杂性理论假设
Standard Covert Security	标准的秘密安全
Standard Model	标准模型
Standard Number Theoretic Assumption	标准数论假设
Standard Reduction-Based Proof Technique	标准的基于规约的证明技术
Standard Worst-Case	标准的最糟情况
Standardized Genus 1 Curve	标准的亏格为 1 的曲线
Standby Database	备用数据库
Start-Up KEK	启动 KEK（密钥加密密钥）
State	状态
State Data	状态数据
Stateful Firewall	有状态的防火墙
Stateless	无状态

State-of-the-Art	技术发展最新水平，当前发展状况，目前发展水平
State-of-the-Art Algorithm	顶尖算法
Static	静态的
Static Adversary	静态敌手
Static Assumption	静态假设
Static Corruption	静态腐化
Static Data Authentication	静态数据认证
Static Group Signature	静态群签名
Static Input Secure Computation	静态输入安全计算
Static Key	静态密钥
Static Off-Line CAM	静态离线凸轮
Static-Secure Garbling	静态安全置乱
Station-to-Station Protocol	站对站协议
Statistical Cryptanalysis	统计密码分析
Statistical Power	统计功耗
Statistical Saturation Attack	统计饱和攻击
Statistical Security Parameter	统计安全参数
Statistical Test	统计测试
Statistical Zero Knowledge	统计零知识
Statistically Secure Steganography	统计安全隐写术
Status Monitoring	状态监测，状态监控
Steganography	隐写术
Stegosystem	隐秘信息系统
Stegotext	隐密文本
Steiner's Algorithm	施泰纳算法
Stochastic Attack	随机攻击

Stochastic Resonance	随机共振
Stop-and-Go Generator	停走生成器
Storage Cost	存储成本
Storage Media	存储介质
Storage Object	储存对象
Storage Server	存储服务器
Straddling Cipher	横跨密码
Straddling Encryption	横跨加密
Straight Line Program	直线程序
Straight Line Simulation	直线模拟
Stream Cipher	流密码
Streaming Delegation	序列式授权
Strength of Mechanism	机制力量
Strict Avalanche Criterion	严格雪崩准则
String Commitment	字符串承诺
String Model	串模型
Strong Authentication	强认证
Strong Context Hiding	强语境隐藏
Strong Diffie-Hellman Assumption	强 D-H 假设
Strong Notion	强概念
Strong Notion of Privacy	强隐私概念
Strong Prime	强素数
Strong Pseudo-Prime	强伪素数
Strong Pseudo-Prime Test	强伪素数测试
Strong RSA Assumption	强 RSA 假设
Strong RSA Based Signature Scheme	基于强 RSA 签名方案
Strong Trapdoor	强陷门

Stronger Variant	强变量
Strongly Biased Linear Approximation	强偏差线性近似
Strongly Unforgeable	强不可伪造
Structural Cryptanalysis	结构密码分析
Structure Preserving	结构保持的
Structured Attribute-Value Data	结构化属性值数据
Structure-Preserving Commitment	结构保持承诺
Structure-Preserving Signature	结构保持签名
STS Protocol	端对端协议
Sturm Sequence	斯图姆序列
Sturm's Theorem	斯图姆定理
Subassembly	组件
Sub-Exponential Number of Bit Operation	亚指数位操作
Sub-Exponential Time	亚指数时间
Sub-Exponentially	亚指数
Subfield	子字段，子域
Subfield Generated by a Subset	由一个子集生成的子域
Subfield Inversion	子域反演
Subfield Operation	分区运算
Subgroup	子群
Subgroup Cryptosystem	子组密码系统
Subgroup Membership	子群成员关系
Subject	面向对象，科目
Subject Security Level	对象安全等级
Subkey	子密钥

Subliminal Channel	阈下信道，潜信道
Subliminal Communication	阈下通信
Sub-Linear	次线性
Sublinear Communication Complexity	次线性通信复杂性
Submodule	子模块
Submonoid	子含幺半群
Subnet	子网络，分支网络
Subordinate Certification Authority	附属认证机构
Subpolynomial Time	亚多项式时间
Sub-Protocol	子协议
Subring	子环
Subscriber	用户，订阅者
Subscriber Registration Model	用户注册模型
Subset	子集
Subset Difference Method	子集差分法
Subset of Members	成员子集
Subset Query	子集查询
Subset Sum	子集和
Subset Sum Algorithm	子集和算法
Subset Sum Problem	子集和问题
Subspace	子空间
Subspaces of a Vector Space	向量空间的子空间
Substitution	替换，代替
Substitution Attack	替换攻击，替代攻击
Substitution Box	代替（S）盒
Substitution Cipher	代替密码
Substitution-Affine Network	代替仿射网络

Substitution-Linear Network	代替线性网络
Substitution-Permutation （SP） Network	代替置换网络
Substitution-Permutation Sandwich	代替置换三明治
Subsystem	子系统，分系统，辅助系统，次系统
Successive Minima	逐次最小
Successive Squaring	逐次平方
Succinct Argument	简明参数
Succinct Multi-Function Commitment	简明多函数承诺
Succinct Non-Interactive Arguments （SNARGs）	简洁的非交互式参数论证
Suite A	程序组 A，套件组 A
Suite B	程序组 B，套件组 B
Sum Construction	求和构造
Sum of Powers Theorem	幂和定理
Sum of Two Squares Theorem	两平方数之和定理
Summation Generator	求和生成器
Sum-of-Square	平方和
Sum-of-Squares Indicator	平方和指示器
Sun Tzu Suan Ching	《孙子算经》
Super Pseudorandom Permutation	超级伪随机置换
Super-Constant	超级常数
Super-Polynomial	超级多项式
Super-Polynomial Helper	超多项式帮手
Super-Polynomial Simulation	超多项式模拟
Super-Polynomial-Time Simulation	超级多项式时间仿真

Superelliptic Curve	超椭圆曲线
Superencryption	超加密
Superimposition	重叠，添上
Superincreasing Sequence	超增序列
Superior Certification Authority	高级认证中心
Superposition	叠加态
Supersession	取代，代替，超级分会，废弃
Supersingular Curve	超奇异曲线
Supervisory Control and Data Acquisition（SCADA）	监控和数据采集系统
Supplementation（Assessment Procedures）	增补（评估程序）
Supplementation（Security Controls）	增补（安全控制）
Supply Chain	供应链
Supply Chain Attack	供应链攻击
Support	支撑，支持
Supporting Service	后援服务，配套服务
Suppression Measure	抑制措施
Surjective	满射的
Surrogate Access	代理访问
SVP	Service Processor 业务处理程序
SV-Robust	SV 稳健
Swap-or-Not	交换或否
Syllabary	音节表
Sylow Theorem	西罗定理
Sylvester's Theorem	西尔维斯特定理
Symbol-Fixing	符号固定
Symmetric	对称的

Symmetric Element	对称元件
Symmetric Community	对称群体
Symmetric Cryptography	对称密码学
Symmetric Cryptosystem	对称密码系统
Symmetric Difference	对称差分
Symmetric Encryption	对称加密
Symmetric Encryption Algorithm	对称加密算法
Symmetric Encryption Scheme	对称加密方案
Symmetric Key	对称密钥
Symmetric Key Encryption	对称秘钥加密
Symmetric Polynomial	对称多项式
Symmetric Proxy Encryption	对称代理加密
Symmetric Proxy Signature Scheme	对称代理签名方案
Symmetric Rational Expression	对称有理表达式
Symmetry	对称
Symmetry of Position	位置对称
Symplectic	偶对的，辛的
Symplectic Base	辛基
Symplectic Geometry	辛几何
Symplectic Transvection	辛变换，平延
Synchronous Communication Model	同步通信模型
Synchronous Crypto-Operation	同步密码操作
Synchronous Stream Cipher	同步流密码
Syndrome Decoding	伴随式译码
Synthetic Data Point	综合数据点
System	系统

System Administrator	系统管理员
System Asset	系统资产
System Categorization	系统分类
System Development Life Cycle (SDLC)	系统开发生命周期
System Development Methodology	系统开发方法
System High	高安全系统
System High Mode	高安全系统模式
System Indicator	系统指示器
System Integrity	系统完整性
System Interconnection	系统互联
System Low	低安全系统
System of Records	记录系统
System Owner	系统拥有者
System Profile	系统概述
System Security	系统安全
System Security Plan	系统安全方案
System Software	系统软件
Systematic Cyclic Code	系统循环码
Systems Security Engineering	系统安全工程
Systems Security Officer	系统安全官
System-Specific Security Control	系统特定的安全控制
Szpilrajn-Marezewski Lemma	Szpilrajn-Marezewski 引理

T

T Method	T 方法
Table Attack	表攻击
Table of Indices	指标表
Table Top Exercise	桌上模拟演习
Tactical Data	战术数据
Tactical Edge	战术优势
Tag	标记，标签
Tag Consistency	标签一致性
Tailored Security Control Baseline	定制的安全控制基线
Tailoring	定制
Tailoring Assessment Procedures	定制评估程序
Tamper	篡改
Tamper and Leakage Resilience	防篡改性和防泄漏性
Tamper Detection	篡改检测
Tamper Resistance	抗干扰
Tamper Response	篡改响应
Tamper-Proofness	防乱用证据
Tamperable	可篡改的
Tampering	干预的
Tampering Attack	篡改攻击
Tandem Daviesmeyer Hash Function	串联 Daviesmeyer 哈希函数

Tandem-DM	串联 DM
Tapping Sequence	抽头序列
Target Collision Resistant	抗目标碰撞
Target Function	目标函数
Target LFSR	目标线性反馈移位寄存器（LFSR，Linear Feedback Shift Register）
Target of Evaluation（TOE）	评估目标
Tarski's Theorem	塔斯基定理
Tate Pairing	Tate 配对
TBAC	Task-Based Access Control 基于任务的访问控制
TC	Time Code 时间码，Terminal Concentrator 终端集线器，Transmission Control 传输控制
TCP	Transmission Control Protocol 传输控制协议
TCPA	Trusted Computing Platform Compliance 可信计算平台联盟
TCR	Tape Cartridge Reader 带匣阅读机，Tape Compiling Routine 带编译常式
TCSEC	Trusted Computer System Evaluation Criteria（美国）可信计算机系统评价标准
TDEA	Triple Data Encryption Algorithm 三重数据加密算法，Taguchi-Differential Evolution Algorithm 田口微分进化演算法
Teardrop	点点滴滴
Technical Control	技术控制
Technical Nonrepudiation	技术的不可否认性
Technical Reference Model（TRM）	技术参照模型

Technical Security Control	技术安全控制
Technical Threat	技术威胁
Technical Vulnerability Information	技术的易损信息
TED	Transferred Electron Device 转移电子元件
Telecommunication	远程通信
Telepass	收费系统
Telescoping Sum	套叠求和法
Teletype Alphabet	电传打字机字母表
Telework	远程办公
Tempest	防信息泄露
Tempest Test	防信息泄露测试
Tempest Zone	防信息泄露范围
Temporary Operating Procedure	临时操作程序
Tensor	张量
Tensor Product	张量积
Terminal Security	终端安全
Ternary Alphabet	三进制字母表
Test	测试
Test Key	测试密钥
Test Plan	试验计划
Tetrahedral Number	四面体数
Tetrahedron	四面体
TGS	Ticket Granting Server 票据许可服务器，Telemetry Ground Station 地面遥测站
Theorem	定理
Theoretical Leakage Resilient Cryptography	理论泄漏弹性密码学

Theta Notation	Theta 记号法
Threat	威胁
Threat Agent	威胁代理
Threat Analysis	威胁分析
Threat Assessment	威胁评估
Threat Event	威胁事件
Threat Model	威胁模式
Threat Monitoring	威胁监控
Threat Scenario	威胁情况
Threat Shifting	威胁转移
Threat Source	威胁源
Threat Vector	威胁矢量
Three-Dimensional Number Shape	三维数形
Three-Round Feldman and Pedersen VSS Scheme	三轮费尔德曼和佩德森 VSS 方案
Threshold	门限
Threshold and Revocation Cryptosystem	门限唤回密码系统
Threshold Authentication	门限认证
Threshold Countermeasure	门限对抗，反测量
Threshold Cryptography	门限密码学
Threshold Decryption	门限解密
Threshold Model	阈值模型，门限模型
Threshold Parameter	阈值参数，门限参数
Threshold Pseudo-randomness	门限伪随机性
Threshold Scheme	门限方案
Threshold Secret Sharing	门限秘密共享
Threshold Security	门限安全

Threshold Signature	门限签名
Threshold Signature Scheme	门限签名方案
Threshold Tracing	门限追踪
Throughput Record	吞吐率记录
Ticket	票据
Ticket Granting Server	票据许可服务器
Tight Bound	紧界
Tight Proof	紧的证明
Tight Reduction	紧规约
Tight Security Bound	安全紧界
Tight Security Proof	紧安全性证明
Tightly Secure Signature	紧安全性签名
Time Bomb	定时炸弹
Time Complexity	时间复杂度
Time Constrained Access Control	时间约束访问控制
Time Stamping	时间戳
Time/Memory Tradeoff	时间/内存的权衡
Time-Compliance Date	时间执行日期
Time-Dependent Password	时间依赖的口令
Time-Lock Puzzle	时间锁难题
Time-Memory Tradeoff	内存时间折中
Timing Attack	定时攻击
Title Registry	标题注册信息
TKIP	Temporal Key Integrity Protocol，临时密钥完整性协议
TLS	Transport Layer Security 传输层安全
TLS Handshake Protocol	传输层安全握手协议
TLS Record Protocol	传输层安全记录协议

TM System	TM 系统
TOE	Tape Overlap Emulator 带重叠仿真器
TOE Security Functions（TSF）	TOE 安全功能
TOE Security Policy（TSP）	TOE 安全政策
Token	令牌
Toomcook Multiplication	Toomcook 乘法运算
Topology	拓扑学，拓扑结构，拓扑
Torsion	扭转，扭曲，转矩，扭力
Torsion Collection	挠集族
Torsion Theorem	挠定理
TOS	Tape Operating System 磁带作业系统
Total Break	完全破解
Total Degree	总次数
Total Risk	全风险
Totally Isotropic	完全等向
Totally Ordered	全序的
Totally Ordered Set（Chain）	完全有序集（链）
Totient Function	欧拉函数
Towering	塔列
TR	Transmitter-Receiver 发送接收机，Tape Register 磁带暂存器，Tape Resident 磁带常驻程式
Trace	迹
Trace Function	迹函数，跟踪功能
Traceability	可追溯性
Trace-Preserving	迹保持
Tracing for Watermarking	水印追踪
Tracing Mechanism	追踪机制
Tracking Cookie	跟踪 Cookie

Tradecraft Identity	间谍情报技术身份
Traditional InfoSec Program	传统信息安全程序
Traffic Analysis	流量分析
Traffic Encryption Key (TEK)	流量加密密钥
Traffic Flow Security (TFS)	通信业务流安全
Traffic Normalization	流量正规化
Traffic Padding	流量填充
Training (Information Security)	信息安全训练
Training Assessment	培训评估
Training Effectiveness	培训有效性
Training Effectiveness Evaluation	培训有效性评估
Traitor	叛徒，泄密者
Traitor Tracing	泄密者追踪
Transaction Pseudonym	事务匿名
Transcendental Element	超越元素
Transcendental Number	超越数
Transform	变换
Transform Mode	变换模式
Transformation	变换
Transient Electromagnetic Device	瞬态电磁装置
Transitive	过渡的，转变的，可递的
Transitive Signature	传递签名
Transitivity	传递性
Translucent	半透明的
Transmission	传输
Transmission Control Protocol	传输控制协议
Transmission Security (TRANSEC)	传输安全

Transparent	透明的
Transponder	应答器
Transport Layer Security (TLS)	传输层安全协议
Transpose of Matrix	矩阵的转置
Transposition	转置，移调，变调
Transposition Cipher	置换密码
Transvection	平延
Trapdoor	陷门
Trapdoor One-Way Function	陷门单向函数
Trapdoor Permutation	陷门置换
Treble Key	三倍密钥
Trial Division	试除
Triangular Number	三角数
Trilinear	三线性
Triple DES	三重数据加密标准
Triple Encryption	三重加密
Trojan Horse	特洛伊木马
Trojan Horses Computer Virus and Worm	木马计算机病毒和蠕虫
Trojan-Horse Attack	特洛伊木马攻击
Truly Password-Based	完全基于口令的
Truncate	删节
Truncated Differential	截断差分
Truncated Version	简化版本
Trust Anchor	信任锚
Trust List	信任列表
Trust Management System	信任管理系统
Trust Model	信任模式
Trust Model Business Control	信任模式商务信控

Trust Relationship	信任关系
Trusted Access Structure	可信接入结构
Trusted Agent	可信代理
Trusted Authority	可信机构
Trusted Center	可信中心
Trusted Certificate	可信证书
Trusted Channel	可信信道
Trusted Computer System	可信计算机系统
Trusted Computer System Evaluation Criteria	可信计算机系统评估标准
Trusted Computing Base（TCB）	可信计算基
Trusted Computing Platform Alliance	可信计算平台联盟
Trusted Distribution	可信分布
Trusted Foundry	可信铸造项目
Trusted Group Authority	可信组特许权
Trusted Identification Forwarding	可信鉴定转发
Trusted Party	信任方
Trusted Path	受托通路
Trusted Platform Module（TPM）Chip	可信平台模块芯片
Trusted Process	可信程序
Trusted Recovery	可信恢复
Trusted Setup	可信设置
Trusted Software	可信软件
Trusted Third Party	可信第三方
Trusted Timestamp	可信时间戳
Trustworthiness	可信性

Trustworthy System	可信系统
Truth Table	真值表
TS	Terminal Series 终端系列，Terminal Service 终端服务，Terminal Station 终端站
TSEC	Three-Speed Ethernet Controller 三速以太网控制器
TSEC Nomenclature	三速以太网控制器命名法
TTP	Trusted Third Party 信任的第三方
Tunnel Mode	通道模式
Tunneling	（网络）隧道技术
Turing Machine	图灵机
Tweak	对……稍作调整，对程序微调
Tweak Size	可调尺度
Tweakable Block Cipher	可调分组密码
Twin Prime	孪生素数
Twin Prime Conjecture	孪生素数猜想
Twirl	旋转扭曲
Twist	扭曲度
Twisted Construction	捻结构
Twisted Edwards Curve	扭曲 Edwards 曲线
Two Factor Authentication	双因素认证
Two Fish	双鱼算法
Two Part Code	两方代码
Two Person Control (TPC)	两人控制
Two Person Integrity (TPI)	两人完整性
Two Tier Hierarchy	两级层级制度
Two to the Kary Exponentiation	2—K 元幂
Two-Key Triple Encryption	双密钥三重加密

Two-Party Computation Protocol	双方计算协议
Two-Party Quantum Cryptography	双方量子加密
Two-Party Secure Computation	双方安全计算
Two-Query Construction	二次询问构造
Two-Round Protocol	两轮协议
Two-Track MAC	双轨道通信协议
Type Accreditation	类型鉴定
Type Certification	类型认证
Type Key	类型密钥
Type of Service Bit	服务位类型
Type Product	类型产品

U

UC Framework	UC 框架
UC-Secure Protocol	通用可组合安全协议
UDP	用户数据报协议
UID	Unique Identifier 唯一识别符
UMAC	Universal Motion and Automation Controller 一种由一套 3U 结构的欧洲标准卡组成的模块化 Turbo Pmac2 系统级控制器
Unauthorized Access	越权存取
Unauthorized Decryption	未授权解密
Unauthorized Disclosure	未授权披露
Unbounded-Depth Circuit	无限深度电路
Unbreakable Code	不可破密码
Uncertainty Principle	不确定性原理
Unclassified	未分级的
Unclonable Function	不可复制功能
Unconditional Authentication	无条件认证
Unconditional Blindness	无条件盲
Unconditional Security	绝对安全
Unconditionally Secure Implementation	无条件安全实现
Unconditionally-Secure	无条件安全
Undeniable Signature	不可否认签名
Undercover Agent Trust	卧底信任
Underlying Scheme	所依托方案

Underlying Semi-Honest Protocol	所依托的半诚实协议
Unforgeability	不可伪造性
Unforgeable	不可伪造的
Unicity Distance	唯一性距离
Uniform Interval Error-Distribution	均匀间隔的误差分布
Unilateral Identity Verification Protocol	单边身份验证协议
Uninvertible Function	不可逆函数
Union	并集
Unipartite Substitution	未分割替换
Unipotent	幂幺的
Unique Factorization	唯一分解
Unique Identifier	唯一识别符
Unique SVP	Unique Service Processor 独特业务处理程序
Unit	单元，单位
Unit Circle	单位元
Unitary	酉，单位的
Unitary Geometry	酉几何
Unitary Operation	幺正（酉）变换
United States Government Configuration Baseline (USGCB)	美国政府配置基线
Univariate Share	单变量份额
Universal	通用的，通常的
Universal Argument	通用参数
Universal Break	通用破解

Universal Circuit	通用电路
Universal Composability (UC)	广义可组合性
Universal Composition Framework	通用可组合框架
Universal Conversion Operation	全称换位操作
Universal Nonlinearity Bound	通用非线性约束
Universal One-Way Hash Function (UOWHF)	通用单向哈希函数
Universal Padding Scheme	全局填充方案
Universal Statistical Test	通用统计检验
Universal Stego System	通用隐写术系统
Universal Verifiability	通用可验证性
Universally Composable (UC)	普遍可组合的
Unlinkability	不可链接性
Unlinkability Property	不可链接属性
Unlinkable Credential	不可链接证书
Unobtrusiveness	非强制性接触
Unrestricted Aggregation	无限制聚合
Unsigned Data	未签名数据
Untraceability	不可追踪性
Untrusted Process	不可信进程
Untrusted Sever	来路不明的服务器
Unveil Phase	揭露阶段
Update	刷新，更新
Update (a Certificate)	更新（证书）
Update (Key)	更新（密钥）
Upper Bound	上界

US CERT	United States Computer Emergency Readiness Team 美国计算机安全紧急响应小组
User	用户
User Authentication	用户认证
User Contingency Procedure	用户应急程序
User Data Protocol	用户数据协议
User Datagram Protocol	用户数据报协议
User ID	用户身份
User Initialization	用户初始化
User Partnership Program (UPP)	用户合作项目
User Registration	用户注册
User Representative	用户代表

V

Valid Data Element	有效数据元
Valid Tag	有效标记，有效特征
Validation	确认，校验
Validity	效度
Validity of Conversion	转换效度
Variable Input Length	可变输入长度
Variable Output Length	可变输出长度
Variable Length	可变字长
Variant	变量
VCC Glitch	虚信道连接短时脉冲波干扰
Vector	矢量，向量
Vector Addition	矢量加法
Vector Decomposition Problem	向量分解问题
Vector Space	向量空间，线性空间
Vector Subspace	矢量子空间
Verifiable	可验证的
Verifiable Computation	可验证计算
Verifiable Computation Scheme	可验证计算方案
Verifiable Database（VDB）	可以验证的数据库
Verifiable Encryption	可验证加密
Verifiable Forgery	可验证伪造
Verifiable Key Word Search	可验证的关键词搜索
Verifiable Mix Protocol	可验证混合协议
Verifiable Proof	可确认的证明

Verifiable Secret Sharing	可验证秘密共享
Verifiable Security	可验证安全性
Verifiable Shuffle	可证明的置乱
Verifiably Encrypted Signature	可验证加密签名
Verification	核验
Verification Algorithm	验证算法
Verification Query	验证查询
Verification Scheme	验证机制
Verified Name	验证名
Verifier	证明者
Verifier Impersonation Attack	验证器模拟攻击
Verify	证明
Vernam Cipher	Vernam 密码
Vernam Table	Vernam 表
Vernam Type	Vernam 类型
Versatile Tool	通用工具
Vertice	顶点
Very Dense Graph	深度密集图
Vicinity	附近
Vigenère Encryption	维吉尼亚加密
Vigenère Table	维吉尼亚表
Vircator	虚阴极振荡器
Virtual Machine (VM)	虚拟机
Virtual Private Network (VPN)	虚拟专用网
Virus	病毒
Virus Protection	病毒防护
Virus Scanner	病毒扫描器
Visual Secret Sharing Scheme	可视秘密共享方案

Voice Recovery	声音恢复
VoIP	Voice over Internet Protocol 网络语音电话业务
Volatile Memory	易失存储器，非永久性存储器
Von Neumann (Shannon) Entropy	冯·诺依曼（Shannon）熵
VPN	Virtual Private Network 虚拟专用网络
VSS	Verifiable Secret Sharing 可验证秘密共享
VSSS	Visual Secret Sharing Scheme 视觉机密分享机制
VTMT	Vulnerability and Threat Management Team 漏洞和威胁管理团队
Vulnerability	易损性
Vulnerability ANA	易损 ANA
Vulnerability ASS	易损 ASS
Vulnerability Impact	漏洞影响
Vulnerability Management	漏洞管理
Vulnerability Scanning	漏洞扫描

W

WAKE-ROFB	网络唤醒，远端唤醒
Walled Garden	围墙花园
Wallet	钱包
Wallet Database	钱包数据库
Walsh Transform	沃希变换，沃尔什变换
WAN	Wireless Area Network 无线区域网
WAP	Wireless Application Protocol 无线应用协议
Warm Site	温站，基于备份的灾难预案
Wasted Performance	浪费性能
Watch List Setup Phase	观察表建立阶段
Watermarking	水印
Watermarking Cryptographic Function	添加水印密码函数
Weak Collision Resistance	弱抗碰撞性
Weak Diffusion Property	弱扩散性能
Weak Hash-Proof System	弱哈希证明系统
Weak Key	弱密钥
Weak Plaintext Awareness	弱密文合法性（又称“弱明文感知性”）
Weak Proof	弱证据
Weak Pseudorandom Function	弱伪随机函数
Weak Security	弱安全性
Weak Session Key	弱会话密钥
Weak Variant	弱变量
Weak-Key Attack	弱密钥攻击

Weak-Key Variant	弱密钥变量
Web Browser Security	网页浏览器的安全性
Web Bug	网页错误
Web Content Filtering Software	Web 内容过滤软件
Web of Trust	信任网
Web Risk Assessment	网络风险评估
Web Scenarios Clients	网络场景里的客户端
Web Security	网络安全
Weddeburn Theorem (on Finite Division Rings)	Weddeburn 定理（有限除环）
Wedge Device	楔形装置
Wegman-Carter Construction	Wegman-Carter 认证术（量子密码学术语）
Weierstrass Equation	魏尔斯特拉斯方程
Weight	权重，加权
Weil Descent	Weil Descent 代数攻击法
Weil Pairing	韦伊配对
Weil's Theorem	韦伊定理
Well Ordering Property (of Natural Numbers)	(自然数字) 良序性质
Well-Ordering Property	良序性质
WEP	Wired Equivalent Privacy 有线等效保密协议
Whirlpool	Whirlpool 哈希算法
White Team	网络模拟攻防规则制定方及裁判
Whitelist	白名单（友好名单）
Whitening	白化变换（Whitening Transformation）
Whitening Key	白化密钥
Wide Area Network	广域网

Wide Trail Strategy	宽径策略
Wide-Pipe Compression Function	宽管道的压缩函数
Wide-Sense Fingerprinting	宽检测指纹
Width-W NAF	宽度 W 非相邻型（W-NAF）算法
Wi-Fi	无线网络
Wi-Fi Protected Access-2 (WPA2)	Wi-Fi 保护访问
Wiki	维基百科网站
Wilson's Theorem	威尔逊定理
Wilt Index	威特指数
Winnowing	风选
Wire Assignment	线路分配
Wired Equivalent Privacy (WEP)	有线等效保密
Wired Equivalent Privacy Protocol	有线等效保密协议
Wireless	无线
Wireless Access Point (WAP)	无线接入点
Wireless Application Protocol (WAP)	无线应用协议
Wireless Door Opener	无线门开启器
Wireless Local Area Network (WLAN)	无线局域网
Wireless Technology	无线技术
Wiretap Channel	窃听信道
Wiretap Channel Scenario	窃听信道方案
Wish List Argument	愿望参数列表
Witness	证据
Witness Hiding	证据隐藏
Witness Indistinguishability	证据不可区分性
Witt's Cancellation Theorem	威特取消定理

Witt's Extension Theorem	威特扩展定理
WLAN	Wireless Local Area Network 无线局域网
Work Factor	工作参数
Workcraft Identity	Workcraft 身份
Working Cryptographer	密码工作者
Working Implementation	实现过程
Worm	蠕虫病毒
Worst-Case Cost	最坏情况成本
Worst-Case Hardness of Problem	最差情况困难问题
Worst-Case Problem	最差问题
Worst-Case Reduction	最坏情况规约
Worst-to-Average-Case Reduction	从最坏情况到平均情况的规约
WPA	Wi-Fi Protected Access 无线网络安全接入
Wreath Product	圈积，环积
Write	写入
Write Access	写访问
Write-Blocker	写拦截

X

X	电抗（Reactance 的符号）
X．509 Certificate	X．509 凭证
X．509 Public Key Certificate	X．509 公钥证书
XACML	Extensible Access Control Markup Language 可扩展访问控制标记语言
XCBC	Extended Cipher Block Chaining Encryption 扩展的密码链块模式，扩展密文分组链接模式
XEDNI Calculus	XEDNI 微积分
XML	Extensive Markup Language 可扩展标记语言
XOR-Cascade	异域级联
XOR-MAC	XOR 消息认证码
XOR-Operator	XOR 运算
XTR	XTR 模拟器（全称 Reflex XTR，德国人开发的一款飞行模拟器）

Y

Yoyo-Game	YoYo 游戏

Z

Zero Divisor	零因子，零除子
Zero Fill	补零，填零
Zero Correlation Cryptanalysis	零相关密码分析
Zero Day Exploit	零日攻击
Zero Knowledge	零知识
Zero Knowledge Argument	零知识论证
Zero Knowledge Interactive Proof	零知识交互式证明
Zero Knowledge Penetration Test	零知识渗透测试
Zero Knowledge Privacy	零知识保密性
Zero Knowledge Proof	零知识证明
Zeroization	归零
Zeroize	填零
Zero-Sum Game	零和博弈
Zig-Zag Exhaustion	曲折衰竭，锯齿形衰落
ZK Sets	ZK 集合
Zombie	僵尸
Zone	区域
Zone of Control	控制区域